A Report of the Center for Counterproliferation Research

Toward a National Biodefense Strategy

Challenges and Opportunities

April 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Toward A National Biodefense Strategy: Challenges and Opportunities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **NDU-WMD Fort McNair Washington, DC 20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**58**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

CENTER FOR COUNTERPROLIFERATION RESEARCH
NATIONAL DEFENSE UNIVERSITY

The Center for Counterproliferation Research has a broad mandate for education and research, and pursues ambitious initiatives in both areas. Through intensive education and outreach programs, including its relationship with the National War College, the NATO Staff Officer Orientation Course, and the Capstone General and Flag Officer Course, the center is dedicated to embedding in military and civilian leaders an awareness of the proliferation threat as it relates to defense policy, programs, and military operations. The research mission includes assessing U.S. counterproliferation policies and programs; developing doctrine and improving training; understanding nuclear, biological, and chemical (NBC) operational and strategic effects; deterring regional NBC adversaries; and enhancing alliance/coalition preparedness and cooperation. Through these efforts, the center furthers the understanding of the evolving security implications of NBC proliferation and fashions effective responses.

A Report of the Center for Counterproliferation Research

Toward a National Biodefense Strategy

Challenges and Opportunities

Center for Counterproliferation Research
National Defense University
Fort Lesley J. McNair
Washington, D.C.
April 2003

Contents

Acknowledgments v

Chapter One
Introduction 1

Chapter Two
The Evolving Biological Weapons Threat 5

Chapter Three
Policy Guidance and the Strategic Context 13

Chapter Four
Homeland Security: Extending the Scope of Biodefenses 25

Chapter Five
Challenges for Defense Planning 35

Chapter Six
Taking the Next Critical Steps 43

Notes 51

Tables

Table 1
Potential Indicators of Biological Weapons Production Facility 8

Table 2
Fall 2001 Anthrax Chronology 10

Table 3
NIAID Biological Diseases/Agents List 30–31

Acknowledgments

The National Defense University's Center for Counterproliferation Research convened a multi-day conference in May 2002 to assess the status of and prospects for a national biodefense strategy. The conference was sponsored by the Office of the Secretary of Defense, the Joint Staff, and the Defense Threat Reduction Agency, and drew widespread participation from each of these and other Department of Defense offices and other Federal agencies and from nongovernmental and industry specialists.

This monograph is grounded in, but further elaborates on, the presentations and discussion conducted in that forum. While all sessions were off the record and all comments delivered on a non-attribution basis, the authors would like to thank the many conference speakers and panelists for their direct and indirect contributions to, and/or review of, this product. In particular, project directors John Reichart, Rebecca Hersman, Jason Ellis, and Richard Love would like to thank the following key participants: Bruce Bennett, Paul Bergeron, Stephen Cambone, Gail Cassell, David Chu, Joseph DiZinno, Lewis Dunn, Barry Erlick, David Franz, Paul Gaffney, Charles Gallaway, Julie Gerberding, Lawrence Gershwin, Steven Goldfein, Margaret Hamburg, Read Hanmer, D.A. Henderson, Paul Jackson, Bernadette Johnson, Anna Johnson-Winegar, Robert Joseph, Rob Kehlet, Ronald Lehman, Robert Mikulak, James Miller, Judith Miller, Donald Minner, Thomas Monath, Tara O'Toole, Vayl Oxford, Stephen Reeves, Gary Resnick, Elizabeth Scharl, and Alan Zelicoff. We would also like to thank Paul Bernstein, David Franz, and Craig Reed for their substantial contributions to this report and Phil Gardner, Forrest Waller, and the rest of the Science Applications International Corporation support team for their considerable and highly effective efforts to organize and implement this large-scale event. Although this product benefited from their active involvement, the opinions expressed herein are those of the Center alone and may not reflect those of any particular conference speaker, the National Defense University, the Department of the Army, or any other department or agency of the U.S. Government.

Chapter One

Introduction

Disease has long been the deadliest enemy of mankind. Infectious diseases make no distinctions among people and recognize no borders. We have fought the causes and consequences of disease throughout history and must continue to do so with every available means. All civilized nations reject as intolerable the use of disease and biological weapons as instruments of war and terror.

—George W. Bush[1]

The United States is re-learning an important lesson in the first decade of the 21st century: adversaries may attack the United States, its interests, or those of friends and allies with biological weapons (BW). The last century witnessed the purported use of glanders by the Germans in World War I and the use of dysentery, plague, and typhus by the Japanese in World War II. But biological weapons were not constrained to wartime settings in the last century. The Rajneeshees, a religious cult in Oregon, employed salmonella to advance their own political agenda. States such as Iraq and the former Soviet Union developed wide-ranging biological warfare capabilities, subnational entities such as Aum Shinrikyo devoted considerable effort and resources to the acquisition of biological agents, and the al Qaeda terror network remains interested in biological capabilities. According to the Director of Central Intelligence, evidence from Afghanistan suggests that al Qaeda was pursuing a "sophisticated biological weapons research program."[2]

The 21st century opened with the startling use of anthrax spread deliberately through the United States mail system, resulting in 5 dead, at least 17 infected, and more than 30,000 on preventative antibiotics. It also led to substantial disruptions in normal activities, the revision of long-standing procedures, and the expenditure of several billion dollars for decontamination efforts.[3] At present, the intelligence community assesses that "approximately" a dozen states maintain offensive BW programs and that interest among particular subnational organizations is high.[4] Looking ahead, current trends will be facilitated and made more complex by the ongoing revolution in biotechnology, the continuing spread of dual-use technologies, the potential for diversion or leakage of expertise, evident weaknesses in international accords designed to prevent BW development and use, and the broaching of the perceived moral barrier against use. Protecting United States forces, facilities, and civilians at home and abroad from biological weapons is a pressing national priority.

The United States requires a national biodefense strategy designed to shape effective policies, guide and maximize investment, and balance competing objectives. Developing such a strategy is a major challenge since the biological threat is complex and highly dynamic. Traditional policy tools for preventing the proliferation of these weapons are lacking. There are significant scientific and technological hurdles to overcome in order to provide effective means of detecting, identifying, treating, and defeating biological agents used as either a weapon of terror or organized warfare. Any national strategy must take explicit account of the biological threat faced by the United States and its allies.

Despite the hurdles, today there is an unprecedented opportunity to forge an effective strategy to defend against biological threats. This unique opportunity is driven by the convergence of high-level attention to the issue, increased resources, public support, and the political will necessary to act. To overcome the threat, the United States requires a comprehensive, sustained, and fully integrated national strategy that engages the national security, public health, intelligence, and law enforcement communities. To be effective, the strategy will require close and effective cooperation across Federal, state, and local levels of governments, between the public and private sectors, with U.S. friends and allies abroad, and with the international community as a whole.

> *Virtually all the equipment, technology and materials needed for biological agent research and development and production are available on the open market as well as in the secondary markets of the world. Vaccine research and disease treatment require essentially the same equipment. Because biological weapons are relatively cheap, easy to disguise within commercial ventures, and potentially as devastating as nuclear weapons, states seeking to deter nations with superior conventional or nuclear forces find them particularly attractive. Therefore BW will probably continue to gain importance since it can kill or incapacitate military forces or civilian populations, while leaving infrastructure intact but contaminated.*
>
> —The Honorable Carl Ford
> Assistant Secretary of State for Intelligence and Research before the Senate Committee on Foreign Relations, March 19, 2002

In May 2002, officials from the White House, Departments of Defense, State, Health and Human Services (HHS), and other Federal agencies discussed their respective efforts at a symposium sponsored by the National Defense University. These officials, together with select nongovernmental and industry specialists, offered insights on the biological threat, policy guidance, operational and response challenges, and evolving programmatic priorities. Included among the many important issues they addressed were:

- The role of treaties and threat reduction activities
- The prospects for deterrence and interdiction
- The role of industry in biodefense
- Preparedness and medical infrastructure
- Military force protection and installation preparedness
- Technical and scientific challenges of detection
- Treatment and forensics
- Military operations in a BW environment.

Conference speakers underscored the imperative of developing a sound national strategy but noted that any strategy must take into account the dynamic nature of the biological threat and the corresponding need for a set of flexible, adaptive resources. A comprehensive strategy will take time to develop fully, both conceptually and in practical terms; not unlike the development of the United States and allied nuclear strategy during the Cold War. The ultimate North Atlantic Treaty Organization (NATO) Cold War-era strategy of flexible response articulated in MC 14/3 was not an agreed alliance strategy until 1968, almost 20 years after the formation of the Alliance.[5] The development and implementation of this strategy represent a useful historical construct:

- The strategic objective articulated in MC 14/3 was to deter the Soviet Union and the Warsaw Treaty Organization through collective defense. Through this strategy, the United States also sought to reassure the NATO allies of its commitment to their security.
    - The objectives of national biodefense strategy must be to prevent the acquisition, development, and use of BW where possible; to protect the United States and its allies against biological attack; to ensure the capability of the armed forces to operate in a BW environment; and to develop the capability to minimize and mitigate the consequences of BW attacks against U.S. interests at home and abroad.
    - The United States must partner with its friends and allies abroad in this effort and enlist the international community as a whole to counter the scourge of bioterrorism and biowarfare.
- The strategic concept articulated in MC 14/3 was flexible response. This Allied strategy called for a spectrum of conventional and nuclear capabilities and options for maintaining and restoring deterrence, including the ultimate sanction of U.S. strategic nuclear weapons.
    - The national biodefense strategy might be thought of as one of comprehensive defense. The strategy will need to address issues ranging from deterrence and preemption, to interdiction and protection, to consequence management and homeland security. This full-spectrum response must harness and integrate public health, national defense, law enforcement, intelligence, and diplomatic tools and capabilities.
    - It will require the effective coordination and leveraging of activities at the international and intergovernmental levels, and the active participation of the private sector.
- NATO strategy was premised on an agreed threat assessment; the 16 member nations of the Atlantic Alliance unanimously agreed to MC 14/3. While member states disagreed at times on the particulars of the threat, the overall nature of the strategic challenge was rarely at issue.
    - The nature of the biological threat, by contrast, is much more difficult to assess. Nations, as well as different national security elements within nations, often disagree on the character, scope, and pace of the BW threat. As a result, it is not a simple matter to develop actionable consensus on how best to contain and counter the threat. Maintaining international focus

on the biological weapons issues is therefore an important element of any U.S. strategy.

- The prospective challenges of biological pathogens and toxins range from their deliberate employment to their natural evolution and global spread. They may be used by actors ranging from mature state-level adversaries, to their surrogates, to the panoply of subnational actors. They may be used against human targets ranging from large groups to individuals, to agricultural targets (livestock or crops), or a range of other targets (for example, bacteria with antimateriel properties). Compounding the evolving BW threat is the ongoing revolution in biotechnology, which, coupled with the continuing diffusion of weapons-related technologies and expertise, may serve to transform the threat from biological weapons in the years ahead. Thus, traditional concerns, for example, the "classical" BW agents, are increasingly joined by emergent considerations such as improvements to existing agents (antibiotic resistance, microencapsulation) and the prospect for "designer" or genetically modified pathogens. Among other things, these developments suggest: the need for a dynamic and adaptive response to an evolutionary problem, acute strategic and tactical warning limitations increase the likelihood of surprise, and the need to develop and sustain effective responses along the entire BW threat continuum, from declaratory policy and public information strategy to medical infrastructure and a robust science and technology base.

The threat posed by biological weapons, while not new, is evolving and does present a series of political, military, technological and psychological national security challenges. While some military and civilian organizations have substantial capabilities in place to help counter the BW threat, others are relative newcomers and have only recently begun to consider their roles in the national biodefense effort. Certainly, the fall 2001 anthrax attacks in the United States triggered an outpouring of resources and captured the attention of the Bush administration as well as the nongovernmental policy community, the media, and the public on BW threats. This monograph assesses the nature of the biological weapons threat and analyzes its broader implications for national security. It articulates the imperative for developing a cogent, robust, and integrated national biodefense strategy and highlights an important set of issues facing the policy, operational, intelligence, and public health communities. Finally, it offers a series of recommendations to understand the changing BW threat and for further developing appropriate responses.

Chapter Two

The Evolving Biological Weapons Threat

Today we know that the scourge of biological weapons has not been eradicated. Instead, the threat is growing. Since September 11, America and others have been confronted by the evils these weapons can inflict. This threat is real and extremely dangerous. Rogue states and terrorists possess these weapons and are willing to use them.

—George W. Bush[6]

The international community faces the growing prospect of emerging infectious disease spread. The potential for deliberate use of biological weapons, however, poses a unique and potentially grave threat to the United States, coalition military forces, and friendly and allied countries. While some of the response infrastructure and requirements will be similar, biological weapons present a distinct set of policy and operational challenges from those posed by chemical, radiological, and nuclear weapons, or even conventional high explosives. To effectively counter the challenge, biological weapons need to be viewed differently from these other threats. Even as the Department of Defense concluded in 1997 that biological weapons would be a "likely condition" of future warfare,[7] this ascendant national security concern is multifaceted and evolving. The underlying trend-line suggests that biological weapons will remain a core security problem for years to come.

A range of potential actors. Much of the recent unclassified literature on the subject focuses on the prospects for, and potential effects stemming from, bioterrorism.[8] Certainly, the public policy community attempted in recent years to size the problem in this context and sought to design a response strategy that would fit a presumptive terrorism challenge. In reviewing the historical record of the 20th century, Seth Carus observes that approximately 25 distinct subnational actors (individuals and groups) have shown concerted interest in biological agents. Eight of these 25 are known to have acquired or developed biological weapons. Only five of the eight are commonly believed to have employed them, and only two have caused significant harm.[9] The fall 2001 anthrax-by-mail attacks should, of course, be added to this list. Yet the biological challenge is far greater than mere subnational actors armed with biological weapons. Terrorism is arguably the lesser-included case. While Milton Leitenberg's assessment that "terrorist use of a BW agent is best characterized as an event of extremely low probability which might . . . produce high mortality" is arguable, his observation that the national debate on the biological threat "is characterized by gross exaggeration, hype, and abstract vulnerability assessments instead of valid threat analysis" is a valid criticism.[10]

Absent appropriate characterization of the threat, it will be difficult to gauge the efficacy or adequacy of any developed response plan.

The Intelligence Community assesses that approximately one dozen states maintain active offensive biological warfare programs.[11] While some of these programs appear to be designed to achieve regional aims, many are either expressly designed for, or would otherwise be capable of, attacking the United States or its interests abroad. Indeed, while much of the recent public policy dialogue focuses on the prospects for bioterrorism, the most serious consequences resulting from the use of biological pathogens or toxins in the near-term are likely to arise from state employment of biological weapons. States generally have substantially greater resources than nonstate organizations and thus are better positioned to acquire larger and more sophisticated biological warfare capabilities. States are more likely to possess the resources needed for the development of novel agents, including exploitation of a greater range of pathogens or creation of genetically modified pathogens that could circumvent existing prevention and treatment mechanisms. Additionally, states are more likely to acquire and exploit technology through the recruitment of scientists associated with the former Soviet biological weapons program. Moreover, many states, including North Korea, Iraq, and Iran, possess multiple means of delivering biological agents on an overt or covert basis.

Of special concern is the prospect that a strategically significant attack could be mounted in the United States without advanced detection using delivery systems operated by special forces, covert operatives, or state-sponsored terrorists. Many proliferant states are known to sponsor terrorist groups that pursue agendas antithetical to the interests of the United States or its friends and allies. This nexus of state-level resources and capabilities and the mass-destruction mindset that particular subnational actors appear to favor lay at the heart of the emerging Bush Doctrine. As Secretary of Defense Donald Rumsfeld testified in May 2002, "we have to recognize that terrorist networks have relationships with terrorist states that have weapons of mass destruction, and that they inevitably are going to get their hands on them, and they would not hesitate one minute in using them. That's the world we live in."[12]

A range of potential effects. Biological weapons range from those capable of creating limited, low-lethality effects to lethal, mass-casualty instruments. They provide a prospective adversary with a diverse set of outcomes ranging from modest disruptive effects to potentially catastrophic physical and/or economic consequences. They may directly target individuals as weapons of assassination or terror, as the former South African program suggests; or they may be intended for large-scale but less lethal effects, as the World War II-era Japanese program indicates; or they may be intended for large-scale effects on human populations or agricultural resources (livestock or crops), as the former Soviet program underscores. They may be fully integrated into war plans or, alternatively, viewed by state actors as a deterrent or guarantor of regime survival.

The materials required to produce biological agents are widely available for use in legitimate activities.[13] Research, development, and production of biological agents are potentially difficult to detect, and in a dual-use context their signatures can often be

effectively masked (see table 1). Similarly, in a post-Soviet and post-apartheid environment, many analysts worry about the fate of the many specialists whose expertise is required for weapons-related development, production, and use. Biological agents can be successfully disseminated via air, water, food supply and distribution, or agricultural systems using overt delivery methods (such as ballistic and cruise missiles, aircraft, or artillery) or a range of covert delivery means (such as sprayers, food or water contamination, or other vectors). Timely detection of disseminated biological organisms is often difficult, and attribution may prove more challenging still. The lengthy incubation period associated with pathogens ensures that the perpetrators of a covert attack can be long gone before the first person becomes ill and awareness of an attack occurs. Moreover, since many biological agents are naturally occurring, it can be difficult to distinguish between their deliberate employment and natural disease outbreaks.

Limitations on warning. While tactical warning is not likely, the Intelligence Community has provided credible strategic warning of extant adversary capabilities or the intent to acquire or further develop biological weapons in the years ahead. The Director of Central Intelligence (DCI) publicly testified in March 2000 that now "more than ever we risk substantial surprise." Frequent (and proficient) deception and denial activities by potential adversaries; the growing availability of dual-use technologies; the increased post-Cold War potential to import specialized talent; and the accelerating pace of technological progress together reduce the prospect of specific warning. Of particular importance is the degree to which the threat "is growing in breadth and sophistication," and how to overcome "significant gaps in our knowledge." In the years ahead, according to the DCI, "rapid advances in biotechnology present the prospect of a new array of toxins or live agents" that may require new detection methods, preventive measures, and treatments.[14]

Preventing specific attacks will result from successful and timely collection, analysis, and dissemination of intelligence data. Yet with respect both to nuclear, biological, and chemical (NBC) proliferation and terrorism, strategic and tactical warnings are prone to failure. Along with an evidently narrowing intelligence collection window, the research, development, and acquisition community has also warned that defenses will lag offenses with respect to chemical and, especially, biological arms.[15] At the same time, understanding adversary capabilities is likely to be considerably easier than accurately collecting, analyzing, and disseminating information on their plans and intentions.[16] Indeed, the states of greatest proliferation concern are also among the hardest intelligence targets; their closed or restrictive political processes often make it difficult to obtain high-fidelity information on such sensitive issues. Information on adversary capabilities, plans, and intentions may not be available, may be fragmentary or misleading, or may change quickly. Uncovering planning documents, informed and current perspectives on special weapons-related issues, or the intentions of key program or senior leaders is a difficult task that ultimately will be only as credible as the human intelligence upon which such judgments are predicated. Among other things, this suggests that the planning, weapons-related research and development, and attack execution advantages go to adversaries, prompting

Table 1. Potential Indicators of Biological Weapons Production Facility

		BW Facility	*Legitimate Facility*
Funding and Personnel		Military/state funded	Private/corporate funded
		High scientist/technician ratio (2:1)	Average scientist/technician ratio (1:6)
		Elite, foreign trained workforce	Mostly domestically trained workforce
		Military/civilian ratio high	Military unlikely
Technical Considerations		Pathogenic strains	Nonpathogentic
		Facilities designed to protect humans from infection	Facilities designed to protect animals
		Facilities designed for decontamination/ disposal of many animals (autoclaves/cremation)	Few animal disposals require decontamination
		Weapons filling equipment	Bottle/vial filling equipment
	Facility Equipment	Access-control badges, security clearances	Badges (minimum)
		Restricted transportation	Public transportation
		Quarantine facilities	No quarantine facilities
		Refrigerated bunkers	Cold rooms in plant
		Aerosol/explosive test chambers	No aerosol chambers
		Rail/heavy truck transportation	Only light truck needed
	Security	Fences, guard towers, patrol roads, cameras, motion detectors, etc.	Little to no outside security
		Military presence	No military presence
Safety		Physical barriers to prevent animal-animal/ animal-humantransmission	Not always present
		Dedicated biosafety and medical personnel	Not always present
		HEPA filters/air incinerators for outflow	HEPA for inflow
		Decontamination showers	Not always present
		Pass through autoclaves (large) and dedicated waste treatment	Small autoclaves and use of common facilities
Process Flow		Raw materials do not match output	Raw materials limited for legitimate products
		Negative pressure	Positive pressure
		Finished products stored in bulk and coded	Product clearly labeled
		Dry product processed in high containment	Milling and other equipment not in containment
		Storage in bunkers, secured, contained, and low temperature	Low security
		Munitions-filling and storage facilities	No munitions
		Testing/proving grounds	Not applicable

Source: U.S. Government, *The Worldwide Biological Warfare Weapons Threat*, 45

the Department of Defense to move away from a "threat-based" planning approach toward a "capabilities-based" planning approach. This capabilities-based approach is central to the 2001 Quadrennial Defense Review: an effort to "anticipate the capabilities that an adversary might employ to coerce its neighbors, deter the United States from acting in defense of its allies and friends, or directly attack the United States or its deployed forces."[17]

The attribution question. The ability to attribute an event involving biological weapons to any individual, group, or state relies heavily on both intelligence and technology. The difficulties associated with timely and accurate attribution are well illustrated with the anthrax letters sent in the fall of 2001. The U.S. mail is collected and distributed in an organized and structured manner. Within a given region, mail is collected and processed by specific postal facilities before being routed to downstream facilities for distribution to the intended recipient. Due to the structured nature of the postal process, Federal investigators have used the delivery addresses and postmarks on the anthrax letters to not only determine a distribution timeline for each letter but to also determine precisely which postal facilities were contaminated by processing each letter. Detection and identification technologies successfully aided in determining which postal facilities the letters contaminated and, working backwards through the postal routing, sorting, and distribution processes, investigators were able to determine from which Princeton, New Jersey, public mailbox the letters were mailed. Yet more than one year later, several critical issues remain unanswered, including when and where the anthrax spores were prepared and who mailed them.

There is no automated technology available today for homeland security use that is capable of detecting and identifying biological agents with sufficient specificity and sensitivity to guide responses. The best available technology for detection of biological agent aerosols involves the use of dry filter units that collect particles from the air over a period of time, followed by transfer of the filter to a laboratory using protocols established by the Centers for Disease Control and Prevention (CDC) Laboratory Response Network. The Office of Science and Technology Policy in the White House has issued guidelines that recommend against the use of field assays due to problems with the specificity and sensitivity of the technologies and systems used. Considerable research and development is under way to develop technologies that could automate part of this process and allow for detection at remote sites. It will probably take a decade to produce such systems suitable for extensive homeland security use.

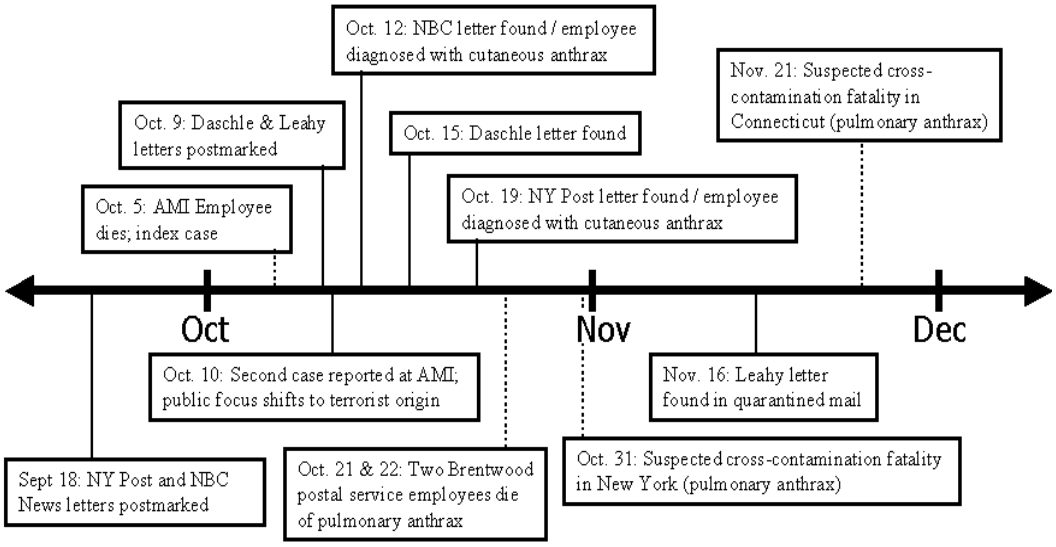
Microbial forensics capabilities remain limited. Armed with limited scientific information, investigators have relied heavily on their time-tested methods of investigation: developing a candidate profile and physically investigating the personal property of those individuals who seem to fit elements of the profile.

A common misconception is that DNA sequence analysis of the spores, when compared to a genomic database, will yield information about who performed the act, just as a fingerprint pulled from a crime scene could identify the perpetrator if that fingerprint can be matched in a database. Although a genetic fingerprint of the anthrax spores will provide information, it will not be the type of information that enables

authorities to attribute the anthrax letters to any given individual. It might, however, indicate where the particular cultures originated, if it proves possible to detect subtle changes in the DNA of different isolates, as in the case of the Ames strain anthrax.

Calibrating the threat. The growing threat of deliberate biological weapons use coexists with concerns about the dangers arising from the natural, and global, spread of new and emerging infectious diseases. For example, diseases such as Korean Hemorrhagic Fever, brucellosis, typhus, and dysentery (among others) are endemic to the Korean Peninsula; some of these have been used or developed by other states as weapons of war. Similarly, anthrax outbreaks in livestock are common in a number of areas, and plague is endemic to regions with strategic importance. As such, it may prove difficult to determine in a timely manner whether a disease was introduced deliberately or accidentally. This underscores that rigidly defined threat lists are not likely to encompass all possible, or even all likely, biological threat agents that the United States and its allies may encounter. To help compensate for evident shortfalls in intelligence, traditional assessments should

Table 2. Fall 2001 Anthrax Chronology



be integrated with robust epidemiological surveillance, environmental monitoring capabilities, counterintelligence, and law enforcement activities. To be effective, these assessments place a premium on effective interagency cooperation, interaction with allies, and appropriate international cooperation. Finally, advances in biotechnology, including the international spread of expertise in the biological sciences, the growing ability to create genetically modified organisms, and the prospects for exploitation of the human and microbial genome projects to create novel agents, suggest that the threat is expanding. While the United States and its allies need to continue their efforts to defend against older, known threats, they must also equip for the potentially expansive threat ahead.

As the United States transforms its conventional military to become increasingly capable, widening its already substantial advantage, aggressor states may increasingly view

biological weapons as one of their few credible means to counter U.S. capabilities. Several countries with offensive biological weapons programs including Iran, Iraq, and North Korea are considered potential military adversaries. These states are developing appropriate delivery systems, including longer-range ballistic and cruise missiles, and could use BW either to attack forward-deployed U.S. or allied military forces or to escalate the risks of military action. They may also employ biological agents clandestinely against forces deploying from or based in the United States or other areas on an "extended" battlefield. They could use or threaten the use of biological weapons against civilian population centers at home and abroad, either to deter the United States or its coalition partners from opposing some act of aggression or to punish the United States or its coalition partners. Hostile states also might target host nations to undermine the ability of the Armed Forces to deploy or operate in forward areas. Finally, adversaries might also threaten or even attack economic targets in the U.S. homeland, notably in the agriculture sector.

Chapter Three

Policy Guidance and the Strategic Context

Biological weapons are a significant threat, and because of the rapidly growing power of biotechnology and biological knowledge, the urgency and the diversity of this threat will only increase. The nature of biological weapons and the epidemics that they could create is such that preventing them will be far more challenging than preventing the catastrophic use of chemical or nuclear weapons. It is going to be hard to detect biological weapons production facilities, it is going to be hard to track the weapons before they are used, and it is going to be very hard to interdict them before they are released.

—Donald Henderson, M.D. MPH[18]
Director, Center for Civilian Biodefense Studies
The Johns Hopkins University

An Emerging National Strategy

The effort to construct a national biodefense strategy must occur within the larger framework of the national security strategy, a principal thrust being countering weapons of mass destruction. The need for a comprehensive national strategy to address the security challenges posed by nuclear, biological, and chemical (NBC) weapons is driven by concern over state programs and the potential for terrorist acquisition and use. In this 21st-century security environment, it is a clear possibility that states or terrorist organizations will seek to use NBC weapons against the United States, forward-deployed assets (such as forces or embassies), or U.S. friends and allies.

The emerging national biodefense strategy is built on three pillars:[19]

- *Proactive counterproliferation efforts* recognize that nonproliferation policies will not solve the toughest NBC challenges. A reengineered set of counterproliferation policies and programs will emphasize proactive interdiction to combat the growing trade in NBC technologies and equipment; deterrence to influence the risk-reward calculus of adversaries; and defensive mitigation to counter operational threats through passive defense, active defense, and counterforce/attack operations.
- *Strengthened nonproliferation efforts* focus on treaties, technology control regimes, and threat reduction programs. The United States will provide political and financial support to nonproliferation treaties, such as the Nuclear Non-Proliferation Treaty (NPT) and the Chemical Weapons Convention (CWC), which seek to advance global and national nonproliferation goals, but will not support conventions whose nonproliferation utility is questionable. Threat reduction programs with Russia are receiving record levels of funding, and increasingly address the BW dimension.

There may also be opportunities to internationalize threat reduction activities so that a broader range of actors and proliferation challenges can be addressed.

- *Effective consequence management* emphasizes managing the consequences of attacks that may occur. The Bush administration created the White House Office of Homeland Security, Congress created the Department of Homeland Security, and Federal organizations from the Departments of State and Treasury to Agriculture and Health and Human Services play a key role in consequent management. At the same time, the Department of Defense is accommodating the homeland defense mission in the organization of the Office of the Secretary Defense and through changes to the Unified Command Plan that established the United States Northern Command (USNORTHCOM).

Any specific strategy or Presidential directive for biodefense must wrestle with the particular challenges posed by biological weapons within these broad policy pillars.

Proactive Counterproliferation

Proactive interdiction. International trade in dual-use technologies is substantial, difficult to track, and hard to control. These proliferation trends suggest new dynamics that in turn require new policy approaches. A growing number of business-oriented networks have emerged in proliferant states. They are of particular concern since they are actively facilitating transactions in NBC-usable materials, technologies, and equipment. Trade in these items is difficult to track or quantify, complicating the assessment of the proliferation impact of these activities, and it is difficult to determine if a single suspected or known transaction represents a significant proliferation threat is challenging. However, there is little debate that weapons-related technologies have become widely proliferated. To avoid a situation in which such trade becomes unconstrained, advance consideration must be given to preemptive peacetime actions to disrupt or prevent the acquisition of dual-use materials by individuals, organizations, or states with known malicious intent.

A proactive posture for interdiction requires a deliberate decisionmaking process that frames policy choices for senior leaders. Such a decisionmaking process must provide the means to assess the significance and risk of particular transactions; identify those that merit U.S. action; recommend specific actions and the political-legal authorities that would legitimate them; and define the expected benefits and costs of possible actions. This process will rely significantly on intelligence that can detect and monitor critical transaction nodes, as well as reliable working knowledge of the structure and status of specific state-run BW programs. The collection of this type of intelligence in support of more robust interdiction strategies is one of the principal challenges facing the intelligence community. An interagency interdiction response group was established to address these and related issues.

The creation of a criteria-driven decision process for peacetime interdiction is a practical approach to address the limitations created by the BW dual-use dilemma: how to determine whether equipment or technologies usable in either civilian or military capacities

is or will be drawn upon for weapons-related activities. Given the stakes, the United States cannot allow this dilemma to be a hindrance to effective action. While there may be no definitive solution to this problem, there is inherent value in deliberate decisionmaking processes that create a sound basis for senior leaders to make difficult judgment calls.

Deterrence. An integrated strategy relying on treaties, technology controls, threat reduction, and interdiction is the first line of defense against BW proliferation. Pursued deliberately and with vigor, such a strategy can be expected to yield some successes. Yet it is important to acknowledge the continued occurrence of BW proliferation and the ongoing erosion of barriers to acquiring bioweapons. Efforts to strengthen deterrence as the second line of defense are therefore imperative. These efforts must proceed from an appreciation of the unique challenges to deterrence inherent in the BW threat.

Deterring state actors. General principles of deterrence still apply when dealing with state actors. The objective is to deter by influencing the adversary's assessment of the expected benefits and costs associated with taking or not taking certain actions. This assessment is driven by the adversary's perception of U.S. capabilities and will to impose unacceptable costs, or by the ability to deny the benefits of the action(s). These principles, however, now exist in a changing landscape in which the principle burden for the United States is not to deter a peer adversary's conventional challenge (as in the Cold War standoff in Europe) but to deter a weaker regional adversary's resort to NBC as a means to overcome U.S. military superiority. If the stakes in regional crises and conflicts are asymmetric in nature, adversaries are likely to be willing to run significant risks and absorb high costs while U.S. willingness to do the same may be unclear. Indeed, since the range of potential adversaries is much broader today, and because there is less mutual knowledge and familiarity, the risk of miscalculation on both sides is high. The United States may believe it has a sound deterrence strategy in place, but may discover that it miscalculated as a crisis or war unfolds.

The 1991 Gulf War exemplifies the uncertainties now inherent in deterrence dynamics.[20] A decade after that conflict, analysts remain divided over the extent to which nuclear deterrent threats were instrumental in Iraq's non-use of chemical and biological weapons. While these threats were the most likely explanation for Iraqi restraint, it is also possible that Saddam Hussein decided not to use these weapons so long as U.S. objectives remained limited to liberating Kuwait. Since the Gulf War ended, it is clear from the statements and memoirs of senior U.S. leaders at the time that the United States had no intention of following through on implied threats to use nuclear weapons in response to Iraqi chemical or biological attacks.[21] Absent a sound working knowledge of the adversary, only a limited basis exists for anticipating with any accuracy an actor's response to deterrent threats. Where there is major uncertainty regarding specific leaders, values, and modes of decision, crafting and communicating deterrence messages is an unpredictable process.[22] The impact of these revelations on the credibility of future U.S. deterrent threats against BW-armed adversaries (not least Iraq) is uncertain but is not likely to make deterrence any easier.

The nature of biological weapons could feed any doubts an adversary had about the credibility of U.S. deterrent threats. For instance, an adversary may believe he can use bioweapons in a way not possible with chemical or nuclear weapons to mount a strategically significant attack that remained below the threshold of a decisive or devastating U.S. response. It is not clear whether likely adversaries will possess the sophistication to fine-tune the employment of BW in this way, but believing it possible may alone be sufficient to weaken deterrence. Improving the ability to attribute the source of BW attacks is essential to mitigating the risks of such a dynamic and thereby buttressing deterrence. The fact that the U.S. law enforcement community has yet to apprehend the perpetrator of the 2001 anthrax attacks may embolden potential BW-armed adversaries and work against the credibility of deterrent threats.

Deterring BW use may be difficult for other reasons as well. An adversary may plan to use biological agents early in a conflict in the belief these weapons can decisively shape the political, military, and psychological battlefield before U.S. power can be fully brought to bear and perhaps before deterrent threats are fully articulated. Any assumptions that may still exist among policymakers or planners that biological weapons will only be used late in a conflict or as a last resort are likely to contribute to surprise and deterrence failure. When confronting a last-resort situation, the obvious question is how to deter a desperate adversary for whom the stakes in conflict have risen to the highest levels. Here, it will be important to consider how to leave the adversary "something to lose" in order to tilt his calculus toward restraint.

Attaining complete knowledge or understanding of how adversaries may think or behave with respect to BW is unlikely, but efforts to understand and learn more must continue. One of the important tasks ahead is to continually monitor potential adversaries from a deterrence standpoint—their leadership and decisionmaking structures, value systems, deterrence calculus in plausible crisis situations, and strategic-operational thinking on NBC weapons. Institutionalizing such a process will require both traditional and nontraditional means of analysis.

The more that is known about an adversary, the greater the prospect that traditional forms of deterrence will work. But facing large uncertainties, or adversaries believed to be willing to run high risks or absorb high costs, the ability to deny the benefits of BW use grows in importance. This refers to passive and active defenses that support the warfighter, medical countermeasures for U.S. and allied populations, and preparedness to manage the consequences of BW attacks, in particular large-scale events. Conceivably, such measures on their own could have a decisive deterrent effect, though their impact is likely to be greatest in combination with traditional deterrence threats. The synergistic effect of retaliatory threats and highly effective denial capabilities may offer the best prospect for creating strong disincentives for using biological agents. And if deterrence fails, a robust biodefense posture will provide the means to limit the damage caused by any attack. But this will require a highly dynamic biodefense effort that is comprehensive and adequately funded, fully supported by civilian and military leaders and the public at large, and well understood by potential adversaries. This effort must

keep pace with the threat and account for the psychological as well as medical effects of biological attacks on populations.

Deterring nonstate actors and terrorists. The September 11 and anthrax attacks of 2001 demonstrated today's most vexing deterrence question: can terror groups like al Qaeda, if armed with weapons of mass destruction, be deterred from using them? Some analysts argue that the only responsible planning assumption is that "possession=use," that any group possessing such weapons will have no inhibitions in employing them and will not be responsive to traditional deterrence calculations. These groups seek to inflict indiscriminate and large-scale destruction, and, in some cases, may feel great urgency to do so. These nonstate actors lack the tangible assets associated with states against which retaliatory actions can be directed, and they may welcome attacks by the United States as validation of their cause.

While it is prudent to assume deterrence may not work against many nonstate actors, such as al Qaeda, it is also important to consider that the terror threat is not monolithic, and in some cases there may be deterrence leverage points that can be exploited. For instance, a state sponsor or supporter is more likely to be deterred than the terror group itself. Threats directed at states providing territory, material support, or even moral support may be the best way to influence the decision making of a biologically armed terror group. Threats against the leadership of terror groups could have an impact in some cases. Despite their rhetoric, some leaders may not be willing to martyr themselves and might be responsive to retaliatory threats against their persons or their families, and the same could hold true for some operatives.

With respect to bioterrorism, would it be possible to deter such an attack against the United States or its interests if the terror group believed there were effective defenses and countermeasures in place? Even were such measures in place, ensuring that the attackers understood this would be difficult. Some terrorists may be indifferent to their prospects for tactical success. Conceivably, they may be less indifferent to the "blowback" effects of using a contagious biological agent, especially in a regional setting. U.S. information operations could be directed at conveying the risks of such an attack to local populations, including the terror group itself and those it may care about.

In sum, there may be few effective means to deter the most challenging terror groups from using bioweapons. For this reason alone, enhancing preparedness to mitigate the effects of attacks through a comprehensive national biodefense strategy is imperative.

Beyond preventive defense? If the prospects for successful deterrence are inherently uncertain, is it sufficient to put in place effective hedges against the failure of deterrence? Is there a case to be made for not waiting until deterrence fails and adopting a more proactive posture? Fundamentally, the question is whether the limitations of the preventive defense model create risks that are no longer acceptable. The preventive defense construct (prevent threats from emerging through arms control and threat reduction, deter threats that emerge, and defeat threats when deterrence fails) has enjoyed some success but also experienced some failures. In confronting biological threats characterized by highly determined proliferants and the possibility of transfers to terror groups, there is

growing concern that U.S. policy options are limited and that this presents risks that require a more proactive posture. The national security strategy and its companion document on combating WMD articulate such a posture: "Given the goals of rogue states and terrorists, the United States can no longer solely rely on a reactive posture as we have in the past. The inability to deter a potential attacker, the immediacy of today's threats, and the magnitude of potential harm that could be caused by our adversaries' choice of weapons, do not permit that option. We cannot let our enemies strike first."[23]

This posture seeks to prevent or roll back the emergence of biological weapons threats through greater reliance on coercive diplomacy and military action to destroy biological weapons and/or remove the responsible leadership. This posture also seeks to maintain the non-NBC status of former rogue states, which could require sustained political and military engagement. A broad range of actions could fall within this general rubric, from focused operations against critical NBC infrastructure or holdings, to regime change campaigns of lesser to greater military intensity, to monitoring and enforcement actions.

Prospects for success would be highly situation-dependent. Successful coercive diplomacy rests on several variables that are not always present in dealing with NBC-armed rogue states. Focused strikes or other operations directed at discrete NBC targets would benefit greatly from tactical surprise. For operations directed at regime change or of a higher level of intensity, a minimum requirement would seem to be decisive military dominance, including the capability to preempt or otherwise counter NBC use. Of course, the more time the United States requires to prepare a large-scale military action, the greater the opportunity for the targeted country to also prepare, conceal or disperse assets, predeploy operatives, or otherwise make mischief.

Sustained domestic and international political support is equally important. This requires preparing the public and laying the international political and legal groundwork for action. It means forthright acknowledgment of the risks associated with action. Minimizing these risks, which could include adversary revenge use of his surviving NBC weapons, threats to the stability of friendly governments in the region, and antagonizing or radicalizing local populations, will be as important as ensuring the success of any military operations.

Indeed, the degree to which the United States moves beyond the preventive defense model to something more proactive will be a function of how senior leaders assess the risks attending current trends in the proliferation of NBC and the expected behavior of hostile states that possess these weapons. The potential for nondefinitive attribution for a catastrophic NBC event may be an important factor as policy options are weighed. Thus, while the risks of a more proactive posture cannot be minimized, such a posture conceivably may be regarded as the least bad option.

Strengthened Nonproliferation

Biological and Toxin Weapons Convention (BWC). The BWC was established 27 years ago, in recognition of the widely held view that possession and development of biological agents for nonpeaceful purposes should be internationally proscribed. The treaty created a political, legal, and moral norm against such activity that arguably helped

to limit, or at least slow, biological weapons proliferation. Most countries are in compliance with the BWC, but revelations in the 1990s about the Iraqi and Soviet/Russian BW programs raised fundamental questions about the effectiveness of the BWC and its relevance to today's BW threat. The technologies and equipment supporting an offensive BW program are often dual-use and therefore ubiquitous. This is probably the most challenging NBC arms control problem facing the United States. Emerging techniques for genetic manipulation create possibilities that the framers of the BWC could not fully appreciate. There appear to be few effective ways to ensure treaty compliance by states that are determined to pursue bioweapons in violation of their legal obligations.

Since 1994, efforts to strengthen the convention have focused on creating such a mechanism to ensure compliance. The current mechanism is based largely on the elaborate system of declarations and intrusive inspections established by the 1992 Chemical Weapons Convention (CWC). Suggested provisions for a strengthened BWC have emphasized equally elaborate declarations of biodefense, biotechnology, and pharmaceutical facilities, a variety of visits and challenge inspections, and field investigations of alleged BW use or suspicious disease outbreaks. Some of these provisions raised difficult questions for the United States concerning the protection of proprietary commercial data and the potential for intelligence gathering by known or suspect proliferant states. The process intended to strengthen the BWC through a legally binding verification protocol is used by some states (for example, Russia, China, Iran, Pakistan) to attempt to establish loopholes or otherwise loosen existing controls and constraints on materials and equipment that could support an offensive program.

The extensive interagency review conducted by the Bush administration unanimously concluded that the proposed, redrafted BWC Protocol did not serve U.S. interests, was overly reliant on the CWC model, and did not provide optimal tools for monitoring a global ban on biological weapons.[24] Overall, the costs and risks were thought to far outweigh the limited gains in transparency, and policymakers assessed that agreeing to the Protocol could compromise United States biodefense efforts and may expose vulnerabilities. The United States maintains by far the world's largest and most extensive biodefense program. Many allies rely on this program to support or enhance their own countermeasures. Additionally, the provisions were judged to pose a serious risk to U.S. pharmaceutical and biotechnology industries, and may have weakened export control regimes. Based on these objections, the United States withdrew its support from the draft Protocol in July 2001.

At the November 2001 BWC Review Conference, the United States proposed a diverse set of alternative political, military, and public health measures intended to strengthen the BW nonproliferation regime in limited but important ways. These included: stronger export controls, enhanced dialogue among nations on the risks associated with BW proliferation, improved biosecurity for pathogens, biosafety training for personnel, strengthened biodefense efforts, and innovative approaches to improve disease surveillance and the international response to diseases outbreaks. These steps would go beyond traditional arms control measures to address not only the threat posed by

biological weapons, but also the public health and security risks associated with naturally occurring infectious diseases.

In the U.S. view, these and related measures, which can be adopted voluntarily by states or groups of states, are more important than establishing new and legally binding compliance provisions. Such provisions would create expensive new obligations for the vast majority of states that already comply with their existing BWC commitments, whereas some in the administration argue that noncompliant nations would likely avoid the Protocol altogether. Rather, international scrutiny should openly focus on the small number of problem states that have not met their obligations under the existing convention, which is principally a political challenge rather than legal one.

BW threat reduction in the former Soviet Union. In confronting the legacy of the vast industrial enterprises developed in the Soviet Union to research, produce, and field nuclear, chemical, and biological weapons, most attention since the end of the Cold War has focused on nuclear threat reduction. In the last few years, however, political attention and resource allocation increasingly focus on the BW dimension of threat reduction. One endemic problem is the state of physical security at former bioweapons facilities in Russia and former Soviet republics. U.S. teams that have visited these facilities have found serious problems that pose a significant risk of theft and diversion of highly sensitive materials.[25] An important component of the cooperative threat reduction program is to improve physical security and ensure the safe storage of BW-related equipment and materials, and to assist in the dismantlement or conversion of key facilities.

Though site security is a serious issue, perhaps a greater proliferation risk is posed by the large number of unemployed, underemployed, or underpaid Russian scientists with BW-related expertise. This brain drain problem became particularly salient for the United States when information obtained in the 1990s revealed that Iran was aggressively targeting Russian facilities as sources of BW expertise, material, technology, and training.[26] The U.S. response has been to engage these institutes directly within the framework of existing nonproliferation and threat reduction initiatives with the goal of redirecting bioweapons expertise toward activities with little or no proliferation risk.[27] The United States offered to fund joint collaborative research projects on the condition that all contact be terminated with Iran and other state sponsors of terrorism.

The agreement reached with the Russian Federation now covers all major biological research centers (BRCs). The agreement is administered through the existing science centers, which provide a multilateral mechanism for organizing and funding peaceful scientific activities. While attempting to redirect the efforts of those scientists with BW expertise, this bioengagement effort also seeks to create forms of interaction that will promote greater transparency and access, facilitate the interface of Russian scientists into the international scientific community, dismantle and "right-size" the Russian biological weapons infrastructure, improve biosafety and industrial standards, and secure dangerous pathogens.

The expertise required to sustain this program and ensure its success is diverse. The Department of State coordinates the program, which now involves several cabinet departments and agencies, including the Departments of Defense, Energy, Health and Human Services, Agriculture, and the Environmental Protection Agency. Interagency engagement led to a broad range of work in areas related to public health (for example, vaccines and infectious disease treatments, disease surveillance and monitoring), plant and animal health, environmental remediation, and the commercial sphere. Since late 1997, the biological engagement program engaged more than 40 former Soviet Union BRCs and most civilian biological research and development institutes, and funded nearly $100 million in research grants and other programs involving more than 3,500 scientists.

This program faces challenges, including: the need to continually weigh the proliferation risk of specific activities; resource constraints in light of the vast military and civilian biological infrastructure in the former Soviet Union; transitioning from a strictly nonproliferation focus to greater emphasis on commercial self-sustainability; and greater engagement of international partners to reach more facilities and share costs. The challenges may be significant, but the payoffs promise to be substantial not only for nonproliferation and biodefense, but also in leveraging Russian and former Soviet scientific expertise in the area of public health.

Effective Consequence Management

The national security strategy emphasizes the need for effective consequence management to respond to the effects of NBC use. While preventive efforts may succeed, they may also fail. Consequence management is thus a critical third line of defense. Consequence management must be institutionalized in the planning and programming process and be factored into war-planning and concept of operations development and implementation for both the military and civilian communities.

The administration's National Strategy for Homeland Security recognizes the unique risks that biological warfare poses to the United States homeland, regardless of whether the perpetrator is a state, a terror organization, or an individual with an overt or covert agenda. A basic challenge for biodefense of the homeland is to harmonize and consolidate the efforts of many Federal entities across Cabinet departments. The "national vision" outlined in the homeland security strategy entails a range of activities to prevent and protect against biological threats, many of them under the authority of the new Department of Homeland Security, often working in partnership with other Cabinet departments and agencies, as well as state and local authorities. Key biodefense activities include:[28]

- Implementation and oversight of the Select Agent Program to regulate the shipment of certain hazardous biological organisms, toxins and certain genetic materials. More than 300 research laboratories are registered under this program, enhancing the security of pathogens that could potentially be used as terror weapons.
- Creation of a National Biological Weapons Analysis Center to perform and sponsor research in the medical sciences in order to advance the state of knowledge in

areas such as infectious diseases prevention, detection, diagnostics, and forensics. The Center will conduct risk assessments in order to prioritize research and development for vaccines, therapies, and other biodefense countermeasures.

- Development of more, and more effective, medical countermeasures. Emphasis will be on developing new and more effective vaccines and postexposure therapeutics and expanding the stockpile of medical countermeasures.
- Operation of the National Strategic Stockpile (formerly known as the National Pharmaceutical Stockpile and operated by DHS, DHHS, and the VA). This program allows the Federal Government to quickly make available stores of vaccines, antibiotics, and other medical supplies to BW incident sites. The Department of Homeland Security will assist state and local authorities to facilitate the distribution of supplies from the national stockpile.
- Management of the National Disaster Medical System, a Federal/private partnership involving a number of Cabinet departments and agencies. These Federal assets work with volunteer health professionals organized into teams around the country capable of providing rapid and surge disaster medical response to localities.
- Development of a national public health surveillance system to improve prospects for early detection of BW attacks. This will involve monitoring and linking public and private databases on a national scale; providing resources that will allow states and cities to hire more skilled epidemiologists; and strengthening the parallel system for monitoring animal and plant diseases outbreaks.

Challenges and the Way Ahead

Implementing these programs will take time, significant resources, and sustained focus. There is, fortunately, a greater understanding at all levels of government both of the biological threat and of the need for effective, coordinated response policies. Only a few years ago this was not the case. Capitalizing on this newfound attention and understanding to promote consequence management programs should remain a high priority. Strong national-level leadership is vital if proposed programs are to be funded and fully implemented nationwide. Without such support, resource allocation, organizational, and personnel decisions will likely be far more contentious. With an extra $40 billion made available for homeland security programs in fiscal year 2002 and substantial increases (over previous budgets) foreseen, organizations with consequence management missions should be able to redress some of their personnel and materiel shortcomings. Making the most effective use of these funds, of course, will depend on careful planning and programming. Although actions are being taken to enhance needed biodefense and consequence management capabilities, they provide no benefit if not accomplished in time to deter, defend against, or recover from an attack. The development of new equipment, systems, and procedures must be followed by timely and effective implementation.

Difficult challenges as well as important opportunities will present themselves as consequence management programs unfold. Among the key challenges:

- Determining the proper and most effective role for the Department of Defense. Historically, the Department of Defense was the repository for most of the

Nation's biodefense capabilities, including medical research and development and technical response. This is no longer the case. Increasingly, civilian agencies are taking over roles traditionally filled by DOD by default in the past. In this period of transition, however, it is unclear what parts of the response mission will remain with DOD as the Department of Homeland Security is stood up and as HHS continues to improve its response capabilities. Utilizing DOD capabilities for the consequence management mission without detracting from its warfighting mission will require careful consideration. In most cases, the appropriate locus of, and capabilities for, response resides in the civilian sector.

- Maintaining a coordinated public information policy prior to and during an NBC event. The anthrax attacks highlighted significant weaknesses in national response capabilities, which are fragmented between Federal, state and local, and private resources, and were often disconnected even within the Federal Government. The establishment of an Office of Homeland Security within the Executive Office of the President and the creation of a Department of Homeland Security to take the lead in responding to NBC events should help addresses these difficulties.
- Quickly developing capabilities to meet current and emerging threats. Although actions are being taken to enhance needed biodefense and consequence management capabilities, they provide no benefit if not accomplished in time to deter, defend against, or recover from an attack. The development of new equipment, systems, and procedures must be followed by timely and effective implementation.

At the same time, the current environment offers opportunities for biodefense:

- A hallmark of today's homeland security situation is increased funding. The President's fiscal year 2003 budget included nearly $6 billion in funding for bioterrorism response, four times the base funding the previous year. This includes substantial resources for research medical countermeasures and biological detectors, strengthening state and local health departments, and procurement of products for the National Strategic Stockpile. Making the most economical and effective use of these funds, of course, will depend on careful planning and programming.
- Throughout the Federal Government as well as among state and local authorities there is a greater understanding both of the biological threat and the need for effective, coordinated response policies. Only a few years ago this was not the case. Capitalizing on this newfound attention and understanding to promote consequence management programs should remain a high priority.
- The strong support for biodefense and consequence management programs from the Bush administration and Congress, abundantly clear in the former's National Security Strategy, Strategy to National Combat Weapons of Mass Destruction, and National Strategy for Homeland Security Defense and the latter's support for bioterrorism legislative initiatives and increased funding, should not be underestimated. Strong national-level support is vital if proposed programs are to be funded and fully implemented nationwide. Without such support, resource allocation, organizational, and personnel decisions would likely be far more contentious.

Chapter Four

Homeland Security: Extending the Scope of Biodefenses

Without a substantial new federal investment in our public health infrastructure, increased intelligence and preventive measures, expedited development and production of vaccines and treatments, and constant vigilance on the part ofour nation's health care workers, a terrorist attack using a deadly infectious agent whether delivered through the air, through our foods, or by other means could kill or sicken millions of Americans.

—Senator Bill Frist[29]

Protecting the civilian population from the threat of biological attack became the Nation's highest biodefense priority after the terrorist attacks of September 11, 2001, and the anthrax-by-mail attacks that followed. Before that, the majority of attention was devoted to military requirements. Since then, civilian biodefense programs have grown an order of magnitude and now command the vast bulk of national biodefense resources. Organizational and programmatic changes also transformed the domestic biodefense scene. Biodefense was the primary focus of several key legislative initiatives in 2001 and 2002, including the landmark Public Health Security and Bioterrorism Preparedness and Response Act of 2002. This legislation contained provisions to enhance state and local bioterrorism response capabilities, improve management of the stockpile of bioterrorism medical countermeasures, toughen controls on biological agents, and strengthen protections for food and water. The Federal Government revisited the issue yet again at the end of the year in the Homeland Security Act of 2002 creating the Department of Homeland Security (DHS), which assigned significant biodefense responsibilities to the new department. The final architecture, however, is still not in place. The President's January 2003 State of the Union message contained an initiative called Project BioShield to enhance the government's ability to develop and acquire medical countermeasures.

Biodefense funding for homeland security grew dramatically during this period. There was virtually no specific funding for civilian biodefense until 1999, and even in fiscal year 2001 the budget provided only about $300 million. This changed dramatically during 2002. Congress appropriated supplemental funds during fiscal year 2002 that nearly quadrupled national spending on biodefense. Even more dramatically, the Bush administration's fiscal year 2003 homeland defense budget request made defending against bioterrorism one of its four key initiatives. The Federal budget for biodefense

grew to $5.9 billion, almost all the increase devoted to civilian programs. As a result, the center of gravity for biodefense activities is rapidly shifting from the Department of Defense to civilian agencies, especially DHS and the Department of Health and Human Services (HHS).

Medical Countermeasures

Acquisition and development of medical countermeasures has been the primary focus of the homeland security agenda for biodefense since September 2001. This has meant adding existing medical products to the Strategic National Stockpile and developing new ones through a research program at the National Institute of Allergies and Infectious Diseases (NIAID) at the National Institutes of Health. The fiscal year 2004 budget includes nearly $3 billion for biodefense medical countermeasures, including $1.3 billion for pharmaceutical purchases and stockpile maintenance and over $1.6 billion to develop new products. This includes about $890 million to fund BioShield, a 2004 initiative announced in the January 2003 State of the Union message to enhance the Federal Government's ability to develop, acquire, and employ medical countermeasures.

An understanding of the extent of the problem is evident from even a cursory review of the NIAID agent threat list, based on a list prepared by the Centers for Disease Control and Prevention.[30] This list prioritizes the threat to guide countermeasures development. It takes into account the agents' virulence, pathogenicity, contagiousness, route of transmission or likely route of exposure (that is, vector borne or aerosol), environmental stability, and the likely public health impact of agent use.

Strategic National Stockpile. The Strategic National Stockpile, created in 1999 and originally known as the National Pharmaceutical Stockpile, contains stores of antibiotics, vaccines, and other medical countermeasures (including some for chemical and radiological incidents). HHS created the program but executed it jointly with the Department of Veterans Affairs (VA). The stockpile transferred to the DHS, but the other two departments retain a role in its management and operation.

The stockpile operates a dozen 12-Hour Push Packs, each containing 50 tons of medical supplies, which are prepackaged so that they can be delivered immediately by aircraft or tractor-trailer. Supplementing the 12-Hour Push Packs is the Vendor Managed Inventory (VMI), inventories of certain key products held by the commercial supplier of the product for use by the government in the event of a catastrophic attack. Initially, the stockpile focused on antibiotics, but since September 2001 became responsible for ensuring emergency deliveries of smallpox vaccine.

The DHS fiscal year 2004 budget request includes $400 million to maintain the Strategic National Stockpile and nearly $900 million to acquire new medical countermeasures. During the three previous fiscal years, HHS budgeted more than $1.6 billion for the stockpile (including $615 million specifically for smallpox vaccine).

Two key deficiencies undermine the current utility of the stockpile. First, the effectiveness of the stockpile depends on the ability of state and local governments to distribute its contents after delivery. The 2001 TOPOFF exercise, which required a

response to a release of plague, highlighted this problem.[31] While the states have received funding to address gaps in local and state capabilities for responding to public health emergencies, the level of preparedness is highly variable. A second deficiency relates to the contents of the stockpile. It does not contain medical countermeasures for some identified threat agents, and the countermeasures available for some diseases are less than adequate.

The response to the fall 2001 anthrax letter attacks demonstrated systemic progress in providing emergency supplies of antibiotics—something that would have proven considerably more challenging just a couple of years before—but also vividly illustrated the deficiencies in the kinds of medical products available. Because there was no diagnostic test to determine if someone were infected with anthrax, everyone potentially exposed had to be given prophylactic antibiotics to protect them. There was no effective treatment once symptoms were evident in the later stages of the disease. Finally, although the Department of Defense had a vaccine licensed by the Food and Drug Administration (FDA) potentially available for civilian use, the supply was extremely limited due to regulatory issues.

Developing new medical countermeasures. Most of the deficiencies with medical countermeasures require development of new products. Developing such countermeasures has been difficult. In addition to the high costs associated with drug development and testing, it was almost impossible to demonstrate the efficacy of biodefense medical countermeasures. Until recently, FDA approval required a demonstration of efficacy in humans, which would have required exposing people to the biological threat agents. In 2002, the FDA adopted an animal test rule, which will permit a demonstration of efficacy using animal models.

The primary responsibility within the homeland defense arena for developing new medical countermeasures rests with NIAID of the National Institutes of Health in HHS. The NIAID strategic plan calls for development of a wide range of new medical products, including new vaccines, therapeutics, adjuvants and immunostimulants, and diagnostics.

Vaccines. A vaccine is a non-disease-causing preparation that induces immunologic defenses against pathogenic agents. They can provide a defense against pathogens before exposure.[32] For this reason, they also can provide an effective means of protection against antibiotic resistant microbes. Vaccines can be composed of live attenuated (non-pathogenic) organisms, killed (pathogenic) organisms, or purified components of the pathogen such as proteins or DNA.

Although vaccines have a well-established role in military biodefense, their utility in the civilian context is less clear. Experience suggests that it is difficult to ensure people take vaccines, as shown with difficulties in ensuring compliance with childhood immunization schedules. Many existing biodefense vaccines do not offer rapid or long-lasting immunity, exacerbating the compliance problem. Some require repeated doses over a protracted period (weeks to months), and some require annual boosters. Moreover, the civilian population has a more diverse character than military forces, which are typically

composed of health young adults. In contrast, the civilian population includes the very young, the aged, immune compromised individuals (including those infected with human immunodeficiency virus [HIV], under treatment for cancer, transplant patients, and others taking drugs that suppress the immune system). All vaccines cause some side effects, which can in some cases cause permanent injury or even death.

The smallpox immunization program announced by President Bush in December 2001 highlights some of the difficulties in administering biodefense vaccines to civilian populations. Medical experts determined that a significant number of people should not receive the smallpox vaccine—unless exposed to the smallpox virus—because they or someone with whom they have prolonged intimate contact have conditions that put them at higher risk of adverse side effects. Thus, the immunization program will exclude people who have ever had eczema or some other serious skin conditions, who have a disease (such as HIV) that suppresses the immune system, who take medications that suppress the immune system, who are pregnant, or who have one of several other contraindications. Crude estimates suggest that this may cover half of the population. Even with these exclusions, the best available data suggests that one to two people might die and another 14 to 52 people might experience potentially life-threatening illness for every million vaccinees.

Smallpox vaccine may represent a worst case, but it illustrates the complex problems facing use of biodefense vaccines in the civilian context. The research and development process and regulatory approval process for vaccines are time consuming and expensive. Fortunately, numerous vaccine candidates could become available for acquisition within the next 5 years assuming adequate resourcing to complete development. Several vaccines developed by the U.S. Army have languished in Investigational New Drug status for years, and it appears that NIAID intends to use them as the basis for new products. The animal rule also should make possible licensure of certain vaccines that previously would have had difficulty demonstrating the efficacy required to obtain FDA approval.

In the short term, it appears that HHS believes that it can develop replacements for the existing anthrax and smallpox vaccines, and provide new vaccines for botulinum toxin, Ebola, plague, Rift Valley fever, and tularemia. In addition, several government agencies are exploring new adjuvants that are more effective than those currently used. Adjuvants are a component of vaccines that boost the response of the immune system, and are essential to the efficacy of most vaccines.

Therapeutics—antimicrobials and immune modulators. The diversity of agents (known and unknown) necessitates the development of new broad-spectrum antibiotics, antiviral compounds, and immune modulators. One of the biggest problems is that there are few existing therapeutics suitable for use against viral agents, and none have received an FDA license. There is only one antiviral therapy (cidofovir) against smallpox, and its effectiveness is unproven. Scores of other antiviral therapies are under development in the pharmaceutical pipeline, but the overwhelming majority of these have only been developed for use against Hepatitis B and C, herpes virus, and HIV. Currently, only

one broad-spectrum immune modulator exists and it is only marginally effective. The paucity of broad-spectrum immune modulators and antivirals effective against threat agents is a significant deficiency in the U.S. medical countermeasures arsenal.

Nor should we be complacent even with threat agents for which there are effective medical countermeasures. For both pulmonary anthrax and pneumonic plague, commonly available antibiotics such as penicillin, doxycycline, or ciproflaxacin are treatments of choice. Unfortunately, it may be possible to engineer threat agents with resistance to specific antibiotics. The Soviet Union reportedly developed some pathogens resistant to multiple antibiotics.[33] Subsequent scientific advances may make that task easier in the future. Accordingly, we cannot assume that the existing medical countermeasures will be effective against future threat agents.

The NIAID strategic plan calls for developing antivirals effective against smallpox and the viral hemorrhagic fevers, antitoxins for use against anthrax and botulinum toxin, new types of antibiotics targeted against specific threat agents, and monoclonal antibodies that boost immune system response to particular threat agents.

Environmental Detection

Under current conditions, the first indication of a biological attack on a U.S. city is likely to be the appearance of infected individuals at health care facilities. Ideally, it would be possible to detect an aerosol release of biological agents by relying on networks of detectors in every urban area. While tests and limited deployments suggest that it should be possible to develop detection architectures that can support public health and medical responses, the United States is only beginning to develop capabilities in this area.[34]

Many of the existing systems used by the military meet force protection requirements. Although they have some utility for units in the field that are vaccinated against selected bioweapon agents and are trained in chemical and biological defensive techniques, these systems are large, reagent intensive, expensive to maintain and operate, and insufficiently reliable for civilian use. As a result, they are not acceptable tools upon which to base public health response decisions. In contrast to the military requirement, developed for a context in which there are limited laboratory resources available for use by forces in the field, the civilian community can draw on high quality microbiology laboratories available in every part of the country.

Responsibility for developing a robust environmental detection capability to support homeland security efforts will fall to the Department of Homeland Security. Environmental detection will build on previous efforts to develop appropriate environmental detection capabilities suitable for a national system. A first step toward building a national system of this type is BioWatch, announced in January 2003. This system builds on existing technology and relies on dry filter units to collect particulate matter from the air. Because of the inadequacies of automated biological detectors, the samples will be analyzed at facilities belonging to the existing Laboratory Response Network created by the Department of Health and Human Services.

Table 3. NIAID Biological Diseases/Agents List

Category	Agents
Category A Diseases The U.S. public health system and primary healthcare providers must be prepared to address various biological agents, including pathogens that are rarely seen in the United States. High-priority agents include organisms that pose a risk to national security because they: • can be disseminated or transmitted from person to person • result in high mortality rates and have the potential for major public health impact • might cause panic and social disruption • require special action for public health preparedness.	• Anthrax (*Bacillus anthracis*) • Botulism (*Clostridium botulinum* toxin) • Plague (*Yersinia pestis*) • Smallpox (*variola major*) • Tularemia (*Francisella tularensis*) • Viral hemorrhagic fevers (filoviruses [such as Ebola, Marburg], bunyaviruses [such as Hantaviruses and Rift Valley Fever], llaviviruses [dengue], and arenaviruses [such as Lassa, Machupo])
Category B Diseases Second highest priority agents include those that: • are moderately easy to disseminate • result in moderate morbidity rates and low mortality rates • require specific enhancements of CDC diagnostic capacity and enhanced disease surveillance.	• Brucellosis (*Brucella* species) • Epsilon toxin of *Clostridium perfringens* • Glanders (*Burkholderia mallei*) • Melioidosis (*Burkholderia pseudomallei*) • Psittacosis (*Chlamydia psittaci*) • Q fever (*Coxiella burnetii*) • Ricin toxin from *Ricinus communis* (castor beans) • Staphylococcal enterotoxin B • Typhus fever (*Rickettsia prowazekii*) • Viral encephalitis (alphaviruses [such as Venezuelan equine encephalitis, eastern equine encephalitis, western equine encephalitis]) California encephalitis, West Nile Virus, Kysanur Forest Virus, LaCrosse • Food and waterborne pathogens (such as Bacteria [Diarrheagenic E.coli, Pathogenic Vibrios, Shigella species, Salmonella, Listeria monocytogenes, Campylobacter jejuni, Yersinia enterocolitica], Viruses [Caliciviruses, Hepatitis A], Protozoa [Cryptosporidium parvum, Cyclospora cayatanensis, Giardia lamblia, Entamoeba histolytica, Toxoplasma, Microsporidia])

Table 3. NIAID Biological Diseases/Agents List (*continued*)

Category	Agents
Category C Diseases Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of: • availability • ease of production and dissemination • potential for high morbidity and mortality rates and major health impact.	• Emerging infectious disease threats such as Nipah virus and hantavirus NIAID priority areas: • Tickborne hemorrhagic fever viruses • Crimean-Congo Hemorrhagic fever virus • Tickborne encephalitis viruses • Yellow fever • Multidrug resistant TB • Influenza • Other Rickettsias • Rabies

Source: Centers for Disease Control and Prevention, Biological Diseases/Agents List, available at <http://www.bt.cdc.gov/Agent/agentlist.asp>.

The objective over the course of the next decade is inexpensive, reliable, sensitive, and specific environmental detectors that will provide indications of a biological attack. For the present, however, public health experts do not generally have confidence in this technology, and will insist on laboratory confirmation even when field identification technologies are used. The public health community is beginning to address the complexities responding to the results of environmental monitoring. Clearly, false positives are a significant concern given the potential costs associated with a response to a perceived biological attack. Equally important, however, the public health community will need to develop standard operating procedures to identify the appropriate responses for true positives.

Other Areas of Concern

Attribution and bioforensics. The anthrax letter attacks highlighted the critical need by our law enforcement and intelligence communities for timely attribution of biological attacks. Key to such capabilities is a robust bioforensics infrastructure to provide the scientific and technical foundations for investigations. Efforts are under way to develop such capabilities to meet homeland security needs, so that in the future we may be better positioned to tackle such incidents.

Future threats. The biotechnology revolution is reshaping the potential threat even as we construct robust capabilities for responding to the existing threat. The greatest attention has been devoted to concerns that skilled scientists will become able to create

biological agents with enhanced characteristics for use as biological weapons. This might entail improvements in environmental stability or enhanced lethality or the creation of genetically engineered pathogens that circumvent existing medical countermeasures. Similarly, the growing industrial applications of biotechnology may also result in improving production capabilities for biological threat agents. A robust biodefense strategy will need to account for this dynamic threat environment.

The medical system and the public health system: an uncoordinated response network. When the American public thinks of the medical system in the United States they think of high quality medical care provided on demand. The problem with the "medical system" is that it is not a system at all; rather, it is a collection of independent business entities that deliver health care for a fee. Historically, very little funding was devoted to ensuring that the medical and public health systems can respond to and manage a biological weapons contingency. If this shortfall remains unaddressed, it will be a critical point of failure. Success will depend on getting these two communities to work together to communicate effectively to create and agree upon an approach to handling a mass-casualty event.

Enhancing hospital capabilities. Like other business sectors, the business landscape of the hospital industry is so intensely competitive that hospitals do not necessarily communicate with each other nor coordinate their service offerings. In fact, there is no financial incentive to do so. To be maximally profitable, hospitals cut patient capacity, utilize minimal staffing, and operate using just-in-time medical care. The problem with this approach is that at any given time hospitals across the country are operating at approximately 90 percent capacity. Competition is so fierce that approximately 1,000 hospitals in the United States have closed their doors over the past decade due to financial difficulties and industry contraction. Today, the statistics are grim: approximately one-third of all hospitals and half of academic hospitals are losing money. The competitive environment in the health care industry has produced a situation in which U.S. hospitals have almost no surge capacity. In the current environment, it is difficult to determine how to deal with a mass-casualty situation requiring intensive care attention.

In fact, there is no hospital in the United States that is prepared today to suddenly deal with, say, 100 casualties requiring advanced intensive care unit-type care. Further, the competitive and autonomous nature of hospitals means that they do not share information with each other, they do not even practice mass-casualty drills together and, with rare exceptions, have not contemplated the creation of a coordinated response to a local biological event. Consequently, each of the Nation's 5,000 hospitals is too functionally and financially stressed to work as part of a true "system" to assist in the development of the nation's biodefense strategy.

Enhancing disease surveillance. One of the biggest lessons from the events involving the anthrax letters was that clinicians became key decisionmakers on issues not directly related to medicine and human health care. Additionally, local public health officials had an exceptionally difficult time maintaining a continuous situational awareness because they did not have effective communication with the physicians serving

their community. This situation revealed with great clarity that the medical system and the public health system are separate systems that fail to properly interface.

Bearing in mind that medicine and public health, like politics, are local phenomena, the United States is in desperate need of a process that can promote a greater degree of information sharing between physicians and their respective public health agency. Current public health reporting is disease-based and requires laboratory confirmation, a relatively slow process subject to many potential errors due to improper specimen handling. Additionally, physicians and veterinarians rarely report unusual symptoms because the reporting process is both time-consuming and laborious while the consequential public health response is frequently of no use to the practicing physician. For a reporting system to work optimally, physicians need a system that is low-cost, straightforward, and nonintrusive, requiring only minimal time and effort to enter critical information. Ideally, the system would share infectious disease information with all physicians on the system and with higher-level government offices while simultaneously returning guidance to physicians from their local public health agency, as needed. Public health officials, on the other hand, prefer a tool that provides them with continually updated surveillance information as well as rapid notification when a serious disease appears in the community. Statistical tools for analysis should ideally be combined with a means of easy and rapid communication with physicians. Both physicians and public health officials agree that the system should be as low cost as possible, since their budgets are often already fully committed.

Role of research. Developing a civil biodefense plan begins with sound research and analysis. Research is the foundation to understanding the infectious disease processes and in developing effective prevention strategies. With well-funded and effective research, the United States will be best equipped to prevent, detect, and treat diseases whether they arise from natural or deliberate outbreaks and be able to address the numerous gaps in current capabilities. The technology base will be the indispensable driving catalyst behind the development of new pharmaceuticals, medical diagnostics, and environmental detection systems. The vast majority of this research is performed under the auspices of Federally funded programs by legions of scientists and engineers who work in Federal and academic research labs. The basic and applied research performed by these organizations is of incalculable value to the biodefense strategy. Finding ways to energize private sector investments in appropriate research and development should be a key focus of the administration and the Congress.

Chapter Five

Challenges for Defense Planning

Contending with uncertainty must be a centerpiece of U.S. defense planning. Because of the uncertainty about the future strategic environment, this strategy would combine both threat-based and capabilities-based planning, using threat-based planning to address near-term threats, while turning increasingly to a capabilities-based approach to make certain we develop forces prepared for the longer-term threats that are less easily understood.

—Donald Rumsfeld[35]

In the aftermath of the terror attacks of 2001, the biodefense and NBC defense community now face a more demanding set of challenges. The requirement to support the warfighter in preparing for BW operating environments is as important as ever, but the traditional emphasis on passive defense countermeasures is now only one of several key mission areas. Attention and resources must also focus on enhancing installation force protection and supporting homeland defense and civil authorities. At the same time, work must expeditiously progress to further develop appropriate counterforce capabilities and effective attack options. To support all these missions, the acceleration of NBC defense technologies, and enhanced interagency and intergovernmental cooperation, will be essential.

Requirements to defend the homeland against biowarfare and bioterrorism are growing rapidly and may emerge as equivalent in importance and resource allocation to those associated with protecting fielded forces. Because resources are not infinite, senior leaders face a major challenge in determining the appropriate balance in resource allocation between biowarfare defense and bioterrorism defense. It is important to bear in mind that these represent two distinct, but potentially related, biodefense challenges. On the battlefield, the goal is to counter efforts to incapacitate the force and degrade operations. The target may be a largely military population that is healthy, trained, and possibly vaccinated, with at least passive defense measures (detectors, protective gear) at its disposal, and operating under a clear chain of command. By contrast, bioterrorism seeks to create casualties, perhaps on a large scale, in a civilian population that is likely to be urban, of widely varying health and age, unvaccinated and unwarned, less well prepared and equipped, and less clearly responsive to what are multiple lines of public authority. Of course, adversaries may seek to employ terror tactics with biological weapons in war areas in an effort to divert resources or otherwise slow a military campaign, weaken the will to fight, or split a coalition.

In recent months, the Department of Defense demonstrated that defense technologies, equipment, doctrine, and training could be leveraged for the expedient improvement of homeland security. While there are aspects of military biodefense that have application to the protection of civilian populations (as well as agriculture), the defensive templates for these two problems are not one and the same. By the same token, there are presently more Federal resources available than at any time previously. Over the past few years, the DOD contribution has dropped from almost 100 percent to less than 20 percent of total Federal biodefense resourcing. The DOD policy, operational, and investment posture must reflect this reality, with an emphasis on DOD-specific roles and missions.

BW in the Korean Theater of Operations

It is now widely recognized that U.S. understanding of how biological warfare attacks of various types could shape theater warfare is very limited. The Department of Defense only recently began to give more systematic attention to the threat posed by BW to military operations, in particular, the major war plans that guide U.S. preparations for conflict in key regions such as Northeast and Southwest Asia. Analysis and exercise activities such as CORAL BREEZE and DESERT BREEZE have helped combatant commands in these regions gain a stronger understanding of how an adversary's employment of disease agents could affect current campaign plans.

In the Korean theater, for instance, there is now a much greater appreciation of the North Korean BW threat among both U.S. and Republic of Korea (ROK) planners and senior leaders. Any significant North Korean BW attacks, whatever their actual intent, could have serious and widespread military, strategic, and psychological effects, with the potential for high casualties and major operational disruption. Even attacks directed at military facilities such as bases will unavoidably affect nearby populations, creating major, and likely unmanageable, strains on both local health services and those provided by U.S. facilities. Increasingly, many analysts argue that the North cannot achieve its vision of victory on the peninsula without resort to biological warfare. As a result, emphasis has been increased on defensive measures intended to blunt the North's use of BW. To be sure, there remains a great deal of uncertainty about the North's BW capabilities and the plans that would govern their use. But prudent planning needs to anticipate a range of BW attacks that include the following purposes:

- To shape events in Korea, such as efforts to embarrass or inflict damage on the ROK and the United States. For instance, Seoul was acutely concerned about the possibility of covert BW attacks by the North to disrupt the World Cup games in May and June 2002.
- To coerce the ROK and the United States, particularly in the context of heightened political and military tensions.
- To shape the battlefield in the run-up to war through covert attacks, possibly including endemic diseases.

- To support the early stages of an offensive, for example by targeting rear area assets such as ports and airfields.
- To ensure regime survival if the offensive fails.

It is prudent to assume that North Korea's wartime use of BW would be broad rather than discrete, with the goals of breaking the cohesion of mechanized reserve forces, destroying the ROK national political leadership and military command, control, communications, computers, and intelligence structure, disrupting air operations and U.S. force flow into the theater, creating panic and chaos, and pressuring the United States and Japan to disengage. Nor should the on- or off-Peninsula use of contagion be ruled out: Particular agents could be targeted at the ROK, possibly Japan, or the United States homeland if feasible, with the intention of dramatically shifting the political, psychological, and operational landscape before the final victory of the allied powers is achieved.

The challenge ahead is to identify where and how operations are most likely and most significantly to suffer degradation from North Korean BW use, and to develop responsive, risk-based defense and mitigation plans tailored to specific biological agents. Some improved biodefense can be achieved at modest expense, such as enhancing collective protection capabilities at facilities in Korea or issuing low operational impact half-masks. Exercises suggest that doctrinal concepts of operations and tactics, techniques, and procedures may, in many cases, be more important than technology-based solutions in enhancing biodefense. Developing effective procedures to manage the response to a BW attack means being able quickly to apply knowledge developed in advance, for example, about the behavior of BW agents under certain conditions, the profile of daily activities at a specific base, or the collective protection capabilities of specific buildings. It also means being able to rapidly weigh options and implement decisions regarding medical care, evacuation, quarantine and travel restrictions, public affairs, forensic investigation, and related matters.

Air Force Operations in a BW Environment

Doctrinal innovation is important in part because of the recognized limitations in fielded technologies for biodefense, in particular technical detectors. Commanders faced with a known or suspected BW event will have no choice but to respond with the tools that are available to them. Their responsibility will be not simply to survive a BW attack, but to sustain operations despite such an attack. Posturing the warfighter to meet this responsibility requires sound analysis, strong leadership, and the appropriate institutional mechanisms.

As one shifts perspective from the combatant or joint force commander dominant in activities such as CORAL BREEZE to the component commander, operational focus shifts to service missions within the overall war plan. Most recently, the U.S. Air Force began to provide local commanders with guidelines to better prepare for BW threats. These guidelines are a first step toward defining more comprehensive operational concepts for biodefense. In their initial version, they seek to prepare commanders to

make risk-based decisions critical to mission accomplishment and force protection for two core competencies central to any major regional warfighting contingency: logistical throughput and sortie generation. The guidelines provide information to help commanders and staff understand the BW threat and its potential operational impact, prepare for BW events, and execute courses of action in a BW environment. Critical to this process is the effective integration of a range of staff elements, including intelligence, meteorology, NBC defense, medical, mortuary affairs, and public information.

The preparation phase of the guidelines emphasizes the importance of taking actions to reduce the uncertainty surrounding BW attacks and increase the number and quality of options available for responding to an attack. Effective preparation can increase the chances of detecting an attack and reduce its potential magnitude, thereby saving lives. The execution phase of the guidelines focuses on response and mitigation options, the nature of which will be influenced significantly by the way in which the BW event becomes known. This could be early, through intelligence warning, or later, through technical detection, or even later, through medical surveillance or sentinel casualties. Clearly, the earlier that knowledge of a BW attack can be attained, the broader the range of options available to the local commander, and the greater the prospect for minimizing operational degradation.

The Commander's Guidelines for Operations in a BW Environment serve as the point of departure for developing more comprehensive plans, beginning with a prototype base biodefense plan and culminating in a U.S. Air Force counter-BW concept of operations. This guide will reflect recommended changes to doctrine, tactics, techniques and procedures, training, exercises, organization, and programming in areas such as passive defense, active defense, and counterforce. Underpinning this process will be a comprehensive set of operational assessments across Air Force mission areas and major command responsibilities, including site-specific quantitative studies.

Protecting Military Facilities at Home

Enhancing biodefense for the warfighter cannot be limited to the potential theater of operations. In an era characterized by total theater of war and the loss of the concept of a homeland sanctuary, it must be assumed that the Department of Defense is a target on United States territory. Indeed, it is not hard to imagine a resourceful adversary armed with BW deliberately seeking to attack homeland military facilities critical to the generation and projection of large-scale combat power. Successful BW attacks against such bases clearly would also endanger tens if not hundreds of thousands of civilians in surrounding areas.

After the events of September 11, 2001, force installation protection emerged as an important element of DOD chemical and biological defense efforts. DOD initiated a Joint Service Installation Pilot Project (JSIPP) designed to increase chemical and biological defense capabilities at nine diverse DOD sites, facilities that are considered to be particularly important to force generation. The goal is to provide these installations with state-of-the-art contamination avoidance, protection, and decontamination equipment

packages; enhanced emergency response and consequence management capability (to include coordination with civilian first responders); integrated command and control networks; and comprehensive training and exercise plans. These capability enhancements are to be integrated with existing installation force protection and antiterrorism plans. Funded at $56.3 million in fiscal year (FY) 2003, JSIPP will not provide complete protection for the selected sites, but rather is intended to refine concepts of operations and requirements for application across a broader set of DOD installations for inclusion in the FY04 program objective memoranda process.

The JSIPP concept of operations, like that of many other technology demonstrations, emphasizes the integration of new or improved technologies with tailored tactics, techniques, procedures, training, and exercises. Equipment to be provided includes the Portal Shield biological detector and the Ruggedized Advanced Pathogen Identification Device.

Beyond JSIPP, a more comprehensive concept of operations for installation chemical and biological protection must consider preparedness in at least three distinct but related dimensions. First is local response, where the goals are to improve the equipment and training of installation first responders for both chemical and biological attacks, enhance local epidemiology and diseases surveillance to support detection and diagnosis, and provide overseas assigned military personnel, mission essential personnel, and dependents with individual protective equipment. A second tier encompasses theater, regional, and national designated response team assets that would relieve first responders. An important near-term step toward ensuring the availability of dedicated reserve assets will be to fully fund 32 planned NBC Civil Support Teams. These teams would be limited to domestic deployments directed by the state governor. Over the mid- to long-term, consideration should be given to creating specialized active duty consequence management joint task forces. These would be deployable units capable of domestic or overseas response within preestablished timelines. A third and final tier would provide for follow-on support and sustainment capabilities not directly tied to specific plans or preestablished response timelines. These capabilities include technical reachback support; large, fixed site decontamination; pharmaceutical stockpiles for all services; and specialized treatment protocols for hospitals and other health care providers.

Organizational Transformation and Resource Allocation

Investing in biodefense. DOD investment decisions in biodefense are driven by the nature of commercial technological innovation. Civilian markets are now driving many of the technologies that are relevant to long-term biodefense solutions, from information science, to material science, to a range of other science and engineering disciplines. By contrast, the pace of innovation in DOD is relatively slow, and the process for incubating new technologies and transitioning them from lab-to-field is too protracted. This implies some common-sense guidelines for how the DOD expends its biodefense resources.

The bulk of DOD investment for biodefense should emphasize those future, longer-term technologies that are not likely to be the focus of commercial research and development because their applications are largely unique to national security or because they are beyond the planning horizon of the private sector. These technologies will need to emerge from the science infrastructure that supports DOD and other Federal agencies. As they have in the past, these laboratories and science and technology facilities can be expected to develop world-class technologies and applications, and DOD investment should leverage their specialized skills to produce specialized concepts and capabilities. Relatively less investment would go to what may be referred to as gathering technologies, areas of R&D where the demands of the civilian economy assure strong nonmilitary investment. In these areas, robotics, artificial intelligence, power systems, and biotechnology, to name a few, the challenge for DOD is to leverage commercial investment and independent research to meet its needs. This requires a strong dialogue with industry to ensure that DOD interests and needs are understood. Some targeted DOD investments might also be considered to supplement private sector R&D in key gathering technologies.

Finally, near-term requirements for fielded capability can be adequately supported by commercially available technologies developed to serve the civilian market. This includes products of the biotechnology sector that have commercial and other nonmilitary application. While these technologies may not in all cases provide 100 percent solutions to military requirements, with some adaptation they can quickly be applied to provide at least 80 percent solutions that on balance are more operational and cost-effective than systems that are more precisely tailored to military specifications but unavailable in the near-term. Many would argue that it makes sense to accept a modest amount of risk in order to achieve more rapid and affordable improvements to current capability, while directing a larger portion of investment resources to longer-term, more unique solutions. A good example is the ongoing investigation of existing commercial (as well as some military) radars to support the stand-off detection of aerosol clouds.

Joint Requirements Process. The 2001 terror attacks served as a catalyst to restructure the requirements generation and acquisition management process for joint chemical, biological, radiological, and nuclear (CBRN) defense activities. The intent is to increase program responsiveness to emerging defense planning and operational goals by creating a single office within DOD responsible for the planning, coordination, and oversight of CBRN defense operational requirements. This single focal point is a newly established Joint Requirements Office for CBRN Defense, with authority for requirements generation and program objective memorandum (POM) development. In parallel, a Joint Program Executive Office for chemical and biological defense has been created to serve as the single material development and acquisition authority. This will consolidate the current, highly dispersed processes for requirements generation and acquisition management into a more centralized and streamlined structure and ensure that material development activities are truly responsive to requirements.

The new Joint Requirements Office represents the services and combatant commanders in the requirements generation process and acts as their proponent in coordinating and integrating CBRN defense operational capabilities. It performs or supports requirements analyses, develops the POM and related modernization plans, facilitates the evolution of joint doctrine and training, sponsors the development of multiservice doctrine, and coordinates logistics, sustainment, and readiness issues. And in recognition of the expanding missions associated with CBRN defense, the Joint Requirements Office will serve as the single source of expertise for the Chairman of the Joint Chiefs of Staff on not only traditional passive defense issues, but also on matters related to consequence management, installation force protection, support to civil authorities, and homeland defense.

Leveraging DOD capabilities for homeland security. Since the 2001 terror attacks, greater attention is being paid to the ways in which DOD chemical and biological defense capabilities are applied to homeland security and antiterrorism efforts. The mission of the DOD Chemical-Biological Defense Program's mission now includes homeland security and installation force protection, a development that places a greater premium on leveraging traditional warfighter support activities to enhance civilian defense efforts.

Operational support. The anthrax attacks provide a good example of unique DOD operational support to homeland security. The United States Army Medical Research Institute of Infectious Diseases was called upon to perform diagnostics and analysis related to the anthrax-contaminated letters. Originally configured to process 10 samples a month, the Institute's Special Pathogens Sample Test Laboratory actually received, at peak, more than 700 samples in a single day during the anthrax investigation. The Laboratory was able to surge in order to process more than 14,000 specimens between September 11, 2001, and January 2002 to support environmental surveillance, law enforcement investigations, and consequence remediation. Similarly, the Armed Forces Radiobiology Research Institute was tasked to conduct quick-response studies to determine the effects of irradiating mail in order to kill anthrax spores. These empirical tests have provided valuable insights to the U.S. Postal Service and other agencies.

Operational support also includes the insertion of rapid technology for unique civilian defense applications. A prime example is in the area of biological detection. To meet the need for a widely distributed, low-end expedient detection capability, DOD material developers produced the Dry Filter Unit, which samples large amounts of air with a filter that periodically is tested for biological materials. Produced in 45 days to meet an urgent requirement, the system is a good example of a commercial off-the-shelf technology that can be produced in large numbers with no long-lead items and very simple training.

At the higher end of the detection spectrum, DOD was able to create an urban defense version of the prototype Joint Biological Point Detection System developed to support the warfighter. This required using commercial off-the-shelf technology to alter the physical configuration of the deployed system and its technical detection functions to

better suit the urban environment. While not optimized for this environment, this system nonetheless demonstrates the rapid adaptability of some DOD capabilities to provide expedient improvements to homeland defense:

- Current and maturing technologies that are the product of both defense investment and the commercial marketplace can also be integrated for broader biodefense of the civilian population for example, through networked urban surveillance and response systems.
- Scientific Support. DOD research and scientific activities have long played an important role in the development of BW medical countermeasures with civilian application, such as defining new uses for already licensed therapeutics. For example, DOD performed the key studies demonstrating the efficacy of ciprofloxacin as a treatment for anthrax. The Department's unique network of science facilities includes high containment (biosafety level 4) laboratories, live agent test sites, large-scale simulant test grids, and aerosol exposure test chambers.
- Equipment Standardization. Civil-military integration requires the establishment of national standards. In order to ensure standardization and interoperability throughout the response community, DOD co-chairs with the Department of Justice an interagency and intergovernmental board comprised of officials from Federal, state, and local governments that establishes, maintains, and updates a national standardized equipment list to support CBRN counterterrorism planning. This body, the Interagency Board for Equipment Standardization and Interoperability, focuses on technology areas such as interoperable communications and information systems, personal protection, collective protection, decontamination, detection, and medical.
- Tapping Private Sector Innovation. Perhaps unique among Federal agencies, DOD has ready access to a large and diversified private sector industrial base. This industrial base is a major incubator of science and technology solutions to a broad range of national security challenges. In an effort to harness this resource for the war on terrorism, DOD shortly after the terror attacks of 2001 established a Combating Terrorism Technology Task Force to identify innovative technologies to support counterterrorism planning. The Deputy Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense chairs the Task Force working group on Consequence Management and Recovery, which emphasizes commercial off-the-shelf technologies to facilitate rapid fielding of response assets. A Broad Agency Announcement to industry resulted in more than 3,000 proposals related to countering CBRN terrorism. Many came from small businesses, which can take advantage of special programs that encourage the development of promising technologies.[36] Other programs, such as Cooperative Research and Development Agreements, encourage collaborative R&D between Federal laboratories and industry, academia and not-for-profit organizations. DOD also evaluates commercial technologies to determine their maturity and applicability to both military and civilian CBRN defense missions.

Chapter Six

Taking the Next Critical Steps

Our national strategy to combat WMD is based on three pillars. We will pursue robust counterproliferation policies and capabilities to deter and defend against the use of these weapons. We will strengthen nonproliferation measures to prevent states and terrorists from acquiring WMD. We will increase our preparations to respond effectively to any use of WMD against us or our friends and allies. To succeed, we must use new technologies, strengthen our intelligence capabilities, work even more closely with allies, and establish new partnerships with other key states, including former adversaries.

—George W. Bush[37]

The 1991 Gulf War and its aftermath were an important wake-up call that initiated the process of improving prevention and response capabilities to bio logical warfare threats. The 1990s saw incremental improvements in military preparedness and a growing awareness of the vulnerability of the homeland. The terror attacks of 2001 painfully demonstrated that vulnerability in shocking fashion and served as a catalyst to renew efforts to organize for biodefense in a more serious way and on a larger scale. The anthrax attacks in particular highlighted a range of shortfalls related to public information strategy, continuing education and training of first responders, interagency coordination, increased laboratory and diagnostic capability, epidemiological assessment capability, and prepositioned stockpiles of appropriate medical countermeasures. New laws and significant Federal resources are being applied to address these problems, and to their credit, governments at all levels have moved to better understand vulnerabilities and to improve preventive, protective, and responsive measures. Much more remains to be done, and given the complexity of the task, the resource implications, and the high stakes involved, it is essential that future efforts be informed and guided by a clear set of principles and guidelines. This is the principal task for the long haul: to put in place a strategy that is responsive to an evolving threat and comprehensive in harnessing the range of required expertise.

A strategy that is responsive to the threat recognizes that the United States faces a diverse and dynamic set of BW challenges. Biological weapons are increasingly accessible to small groups, though states and state-sponsored terror groups may present the most technically advanced threats. Proliferators are more self-sufficient, sophisticated, and adept at concealment and deception. Specific and timely warning of a hostile biological event is not likely. Both old and new threats must be considered. Many of the known pathogens and toxins harnessed by state weapons programs will continue to be of

concern into the future. The fall 2001 anthrax-by-mail attacks, while small in scale relative to the range and type of potential biological attack scenarios, revealed the kinds of problems associated even with traditional agents assumed to be well understood. From diagnostic difficulties, treatment uncertainties, and the inconsistent and sometimes contradictory nature of government responses, to the still unresolved question of attribution, the first 21st-century biological attack on U.S. soil has forced a reexamination of the conventional wisdom about disease agents against which the United States has long planned. At the same time, the biotechnology revolution likely will result in a qualitatively different threat over the next 15 years, characterized by advances such as microencapsulation, antibiotic resistance, and designer pathogens or other genetically modified organisms.

In this light, the 1990s-era validated threat provides an inadequate basis for developing the range of countermeasures that will be required to hedge against a future surprise. As a basis for planning, the evidentiary is too limiting, but the possible is simply too broad.

This has at least two important implications for strategy. First, there is a clear need for a risk-based approach that complements the threat validation process with rigorous analysis and red-teaming to identify and direct resources toward the most serious threats deemed to be sufficiently plausible or likely. Scientists and planners must have the flexibility and the resources to think systematically about non-validated threat agents. Developing consensus and making choices about which traditional and emerging threats to prepare for is not an easy task. But it is unrealistic to attempt to protect against every threat possibility. As risks are systematically assessed, it should be possible to make decisions about the degree to which specific threats can and cannot be accepted. While some threats may need to be eliminated entirely, others can be reduced or mitigated, while still others may pose an acceptable risk in light of higher priorities.

Recent decisions regarding anthrax and smallpox highlight some of the choices confronting decisionmakers as they attempt to calibrate risk for purposes of resource allocation. Vaccinating some deploying forces (and in the case of smallpox, some first responders as well) reflects prudent concern about the risks posed by these high-consequence threat agents. But there may be other high-consequence agents that also merit resources (such as Marburg or other viral hemorrhagic fevers). In turn, it may make sense to devote relatively fewer resources to other threat agents that are arguably more difficult to use on a mass scale, such as ricin. A resource allocation strategy that privileges the more consequential threats, if not perhaps the most likely, might help diminish the appeal of biological weapons. Over the longer term, substantial investment should be made to develop safe and effective multivariant vaccines, antivirals, and broad-spectrum antibiotics against the full-range of known or classical threat agents.

A second implication is that the dynamic nature of the threat means engaging in a number of biological weapons arms races with multiple potential adversaries, both foreign and domestic. These adversaries have certain advantages in their pursuit of offensive BW capabilities, including the availability of dual-use technologies, possible access to personnel and material from the former Soviet Union, ease of concealment, and a

number of potential delivery means. Winning these multiple BW arms races will not be easy, since precisely identifying adversary capabilities may be impossible. But getting and staying ahead of the threat means that U.S. biodefense strategy must aggressively exploit unique competitive advantages—technological prowess, a culture of innovation, financial resources, adaptive armed forces, and a position of global leadership.

A comprehensive strategy recognizes from the outset the need to mobilize the nation's resources in ways that transcend traditional boundaries. Biodefense strategy spans the diplomatic, national security, public health, and law enforcement domains. The strategy must engage government at all levels, and government must in turn establish effective partnerships with the private sector. In the continuum of biodefense strategy, one focal point is on political and security measures required to attack the legitimacy of BW use, prevent further proliferation, reduce existing threats, deter BW-armed adversaries, and protect warfighters and others essential to military operations. A second component of the biodefense continuum emphasizes public health measures to provide medical protection to civilian populations through vaccine and treatment programs and to ensure preparedness to respond to the deliberate use of disease agents in the United States. A final element focuses on protecting against and responding to threats to the U.S. agricultural sector, which have the potential to create severe stress and damage to the economy on a massive scale.

Connecting these elements into a cohesive national strategy is a major political, organizational, and resource challenge. In this process, there is no alternative to building institutional relationships at the interagency and intergovernmental levels, engaging the public, and fostering a community of public and private expertise serving the national interest. The challenges of Cold War deterrence and containment led to the creation of a community of theorists and practitioners that helped chart the course of national security for over two generations. Today, the biodefense community faces no less a challenge in marshalling very diverse expertise, at home and abroad, to defeat or contain an even more complex type of threat.

The prevention elements of biodefense strategy require new thinking and innovative approaches. The limitations of traditional biological weapons arms control require prevention to be pursued through less traditional, more innovative means. The United States is attempting to do this through the Biological Weapons Conventional review process and ongoing cooperative threat reduction programs with the states of the former Soviet Union. Making Russia part of a wider biodefense strategy is imperative; both to reduce proliferation risks and to leverage Russian expertise to better understand biological weapons threats, countermeasure, and public health strategies.

In light of the unique characteristics of biological agents, deterrence of biological warfare is problematic in an era of asymmetric conflict and high levels of uncertainty about how and when adversaries may employ BW. Keys to successful BW deterrence include at least the following:

- Institutionalizing a process to continually monitor potential adversaries from a deterrence standpoint

- Developing declaratory policy and posturing considerations tailored to specific actors
- Improving the ability to attribute the source of BW attacks
- Complementing traditional deterrence threats with robust denial and defense capabilities.

Given the uncertainties surrounding deterrence, greater emphasis in biodefense strategy must be given to proactive interdiction to better control the trade in technologies and materials that can advance offensive BW programs.

Enhanced protection for warfighters rests on preparing commanders and troops for biological attacks and fielding improved biodefense systems. Field commanders need to be provided with low-cost, procedure-based guidelines to support operational planning and execution of biodefense measures. This is a first step toward developing more comprehensive biodefense operational concepts, informed by careful assessment of how warplans and operations in specific theaters of conflict are likely to be affected by adversary use of biological weapons. In the near- and mid-term, fielding effective biodefense systems requires leveraging available commercial technologies, even if these do not provide 100 percent solutions. Over the longer term, the bulk of DOD investment should be in technologies that are unique to national security or beyond the planning horizon of the commercial sector. These technologies leverage the specialized skills of the science and laboratory infrastructure that support DOD and other Federal agencies.

The dynamic nature of the threat means that the United States is engaged in a number of biological weapons "arms races" with multiple potential adversaries, both foreign and domestic. These offense/defense adversaries have certain advantages in their pursuit of offensive BW capabilities, including the availability of dual-use technologies, possible access to personnel and material from the former Soviet Union, ease of concealment, and a number of potential delivery means. Winning these multiple BW arms races will not be easy since identification of an enemy's capabilities may not be possible. But getting and staying ahead of the threat means that United States biodefense strategy must aggressively exploit unique competitive advantages—technological prowess, a culture of innovation, financial resources, adaptive armed forces, and a position of global leadership.

Prepare for the Full Range of Plausible Threats

Countering the "oldie-moldies." The wide range of plausible threat agents suggests the need for an expansive approach to biodefense. Particular state actors have successfully weaponized a range of classical viral and bacterial pathogens and toxins. While recent progress has been made in effective prophylaxis for smallpox and anthrax, a robust defensive strategy needs to prepare for the full range of known threat agents. Indeed, while the decision to vaccinate forces deploying to high-threat regions against these two high-consequence agents (and to recommend that first responders be inoculated against the former) is a sound starting point, care must be taken to ensure that these biodefense efforts do not eclipse other needed actions. In the near-term, resources should be made available for other potentially high-consequence threat agents, such as Marburg or other

viral hemorrhagic fevers. At the same time, lesser attention can be paid to other potential biological agents, such as ricin, which is arguably more difficult to use on a mass-casualty basis yet continues to garner scarce resources of potential adversaries. A resource allocation strategy that privileges the more consequential threats, if not perhaps the most likely, might help diminish the attractiveness of biological weapons. Over the longer term, substantial investment should be made to develop safe and effective multivariant vaccines, antivirals, and broad-spectrum antibiotics usable against the full range of known or classical threat agents.

In addition to increasing stockpiles of existing and fielding new medical countermeasures, efforts to develop and implement more effective concepts of operation must be made. In the military arena, this suggests building, as appropriate, on the Air Force's emerging counter-BW operational concepts; on doctrinal advances led by the Joint Requirements Office; on improved war-planning in regional combatant commands; on increased training relating to the full range of operations in a BW environment, from passive defense through attack operations; on improved defensive measures at U.S. bases at home and abroad; and on fine-tuning support to civilian communities, leveraging unique DOD capabilities while preserving the Department's ability to execute its core warfighting responsibilities. In the civilian context, this suggests fine-tuning existing interagency crisis and consequence management planning; a more robust training regimen and exercise schedule at the Federal, state, and local levels; increased stockpiles of prophylactic countermeasures against a range of plausible threat agents; the development of additional laboratory analysis capabilities, and requirements for attribution of a biological attack; and continuing education of senior officials, media representatives, first responders, and the public as a whole. For each community, building on existing medical infrastructure, epidemiological surveillance networks, detection technologies, and medical countermeasures will yield considerable dividends.

Emerging technologies and genetically modified organisms. Emerging technologies from the biotech industry, the national labs, and academic facilities will unintentionally but inevitably enable the development of sophisticated malicious applications of biotechnology. Reports are in abundance in the press and in peer-reviewed publications about scientists' demonstrated ability to convert nonpathogenic organisms into pathogens. Genetic engineering allows for the swapping of virulence genes and pathogenicity elements between organisms, creating pathogens of increased virulence, infectivity, and different host ranges. Intellectually, it is not a big step to apply these same techniques to create organisms more resistant to treatment, or organisms that are capable of circumventing vaccines or evading current detection technologies.

The game of developing agents more resistant to defenses versus the development of defenses more resistant to agents is one of increasing escalation of measures versus countermeasures. To be successful, biodefense must be able to take greater advantage of emerging biotechniques to develop countermeasures capable of overcoming genetically engineered agents. Scientists must actively think through a range of offensive scenarios involving biological weapons and use these as guides for the development of

effective countermeasures against the unknown. To do so, the Department of Defense and other Federal agencies must have the ability to apply significant resources against nonvalidated threat agents. While the "oldie moldies" remain viable threats, planning and resource allocation must appropriately consider advances in biotechnology that have the potential to transform the current threat equation.

Threats to agriculture must be addressed. Biological attacks against U.S. agriculture are capable of massive economic damage. Agriculture constitutes a $1.3 trillion sector of the national economy, accounting for 13 percent of GDP and 1 in 6 jobs. It is therefore a lucrative target, especially to adversaries following a strategy of "exhaustion" intended to damage the U.S. economy and impose large financial and societal costs. It is also a vulnerable target, receiving far less attention than other critical "networks" such as civil aviation, maritime commerce, and information infrastructure. Intensive farming practices in the United States have contributed to keeping food prices low due to economies-of-scale. These same practices that keep consumer prices low—raising animals and plants in highly concentrated environments—are at the root of U.S. vulnerability. For example, in the livestock industry 2 percent of United States feedlots produce 78 percent of all United States cattle and the 40 largest swine producers generate 90 percent of the pigs in the United States market. This situation is similar to that in the agricultural industry where vast expanses of crop monocultures such as corn and wheat are planted across the midsection of the United States. These practices significantly increase the likelihood that an infectious disease outbreak will rapidly spread great distances and decimate a particular crop or animal population.

Unfortunately, matters of agroterrorism have not been afforded the same degree of Federal support as matters directly affecting human health. Yet estimates of agricultural bioterrorism demonstrate that it would be relatively easy for an individual to inflict significant economic damage on the United States with minimal risk to the perpetrator. For the most part, agricultural contagions would be easy to introduce since they pose little risk to the perpetrator. Additionally, sophisticated dispersion equipment may be unnecessary since some livestock and poultry diseases can be transported between farms on contaminated footwear and feed trucks and may even be capable of traveling on the wind. After the fact, attribution would be difficult, if not impossible, since the deliberate introduction of a disease may be indistinguishable from an accidental introduction or a natural outbreak.

The United States public, press, and politicians are unprepared for the draconian control measures that would occur if a foreign animal disease outbreak such as foot and mouth disease (FMD) were to occur in the United States. The psychological impact of graphic images depicting the mass slaughter of animals in trenches miles in length cannot be underestimated. Projections of the impact of an FMD outbreak in the United States suggest that the situation here could be significantly worse than the events that occurred in the United Kingdom in 2001. This is due in large measure to the densities and concentrations in which livestock are housed. The financial impact of such an event is not limited to the

cost of animal disposal and disease eradication efforts; this is typically only a fraction of the revenue lost to disrupted production and trade.

Improvements in surveillance, infrastructure, and communications are key. Biotechnology will drive the biological weapons threat and must also drive the development of countermeasures and defensive capabilities. The research base is thin and there is a pressing need for sustained, laboratory-based research in the areas of pathogenesis, genomics, vaccine processes, combinatorial chemistry, and many other disciplines to ensure a sufficient science and technology base for understanding threat developments, defining practical solutions, and hedging against surprise. Accelerating the laboratory-to-field transition—whether for civil or military application—will require streamlined acquisition and regulatory processes. While adequate levels of public investment are essential, this will not be enough. The government must find ways to harness innovation in the private sector and academia. Fortunately, much of this research can have a near simultaneous benefit for the public health and in the battle against naturally occurring infectious disease. Finally, the United States must invest in people to ensure robust research and continued innovation. Expertise today does not run deep enough. A sustainable biodefense strategy requires a national initiative to ensure a well-trained, highly motivated cadre of specialists.

Strengthen—and better connect—the Nation's medical and public health infrastructures. The medical response infrastructure today is poorly prepared to respond to major biological events. Surge capacity is a major problem—a direct result of the "just-in-time" business model. Hospitals in the United States lack the incentives, networks, facilities, and personnel to prepare individually or collectively for complex biological events involving large-scale casualties. The competitive, autonomous nature of hospitals means there is little information sharing to support surveillance, few joint mass-casualty drills, and limited efforts to develop a coordinated response to a local biological attack. Moreover, the disaster response template for hospitals is based on the treatment of trauma injuries, not contagion or sustained emergency treatment of disease.

At the same time, there is significant erosion in the Nation's public health infrastructure, due in part to inadequate public investment. The response to the anthrax attacks demonstrates one inevitable result: medical clinicians in emergency rooms and private practice, as opposed to public health officials, were key decisionmakers on issues not directly clinical in nature, such as the creation of data-sharing networks and responses to public anxiety. Local public health officials found it difficult to maintain situational awareness due to poor communication with local physicians. This situation demonstrated the degree to which public health care and medical systems are separated by inadequate communication and interaction.

Too little attention is being paid to these problems, and too little investment is being made to correct them. There needs to be a central organizing hospital authority at the local, state, and/or Federal level to provide guidance and direction to all hospitals resulting in a coordinated plan for the medical community to follow in response to bioterror events. State health departments may be an excellent starting

point for determining and assigning local and regional responsibilities. This may be one way in which to strengthen the linkages between the public health and medical systems. Another may be through improved surveillance practices, in particular automated systems designed to facilitate timely sharing of infectious diseases information. If endemic weaknesses in the public health infrastructure are not remedied, then national strategy will increasingly rely on clinicians as the front line of domestic biodefense. If this occurs, resources directed to incentivize the medical system to improve health monitoring, disease surveillance, and overall preparedness for BW events will continue to lag. Some observers suggest that the anthrax experience demonstrates that this approach will not work.

Confidence in government medical information and advice must be restored. Confidence in governmental medical advice is eroding. It is hard to imagine an effective biodefense strategy without a concerted effort to restore credibility and trust. A comprehensive public education program is required to build scientific literacy and public understanding at the Federal, state, and local levels through accurate information and a careful discussion of risks. The program should involve recognized experts who can communicate factual information clearly and without condescension. Such a program is needed now, not during or after a crisis when the public may be more agitated and less receptive. A policy such as the Bush administration's December 2002 recommendation that first responders receive the smallpox vaccine, for instance, will ultimately be only as successful as its implementation at the local level.

Look to History in Developing Biodefense Strategy

Finally, the United States successfully marshaled national will, expertise, and resources in the past to confront serious new threats to the Nation's welfare. There may be useful lessons from past strategies that can inform current efforts to articulate and advance a national biodefense strategy. For example, NATO's Cold War strategy of "flexible response," while directed at a different threat in a unique political-military setting, incorporated many important features of a successful strategy. It had a clear policy goal that was easily described and understood. It was based on a sober and continually updated assessment of threat and warning assumptions. It relied on a range of capabilities to complicate the adversary's planning and encourage restraint. It institutionalized strategy planning and execution, including the allocation of resources. And it drew on the thinking and analysis of a community of experts in and outside of government. Strategy attributes of this kind can serve as guideposts as the United States develops a comprehensive plan to counter the biological warfare threat that is critical to both national and homeland security in the years ahead.

Notes

[1] White House, Statement by George W. Bush, "Strengthening the International Regime against Biological Weapons," Office of the Press Secretary, November 1, 2001.

[2] George J. Tenet, testimony to the Senate Select Committee on Intelligence, February 6, 2002, 3.

[3] Center for Counterproliferation Research, *Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks* (Washington, DC: National Defense University, November 2002), 1–12.

[4] George J. Tenet, testimony to the Senate Foreign Relations Committee on "The Worldwide Threat in 2000: Global Realities of Our National Security," March 21, 2000. See also Thomas R. Wilson, statement for the record to the Senate Armed Services Committee, March 19, 2002.

[5] North Atlantic Military Committee, "Final Decision on MC 14/3: A Report by the Military Committee to the Defence Planning Committee on Overall Strategic Concept for the Defense of the North Atlantic Treaty Organization Area," January 16, 1968. This section draws on a working summary of conference proceedings prepared by Lew Dunn, May 30, 2002.

[6] White House, statement by George W. Bush, November 1, 2001.

[7] Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Government Printing Office, September 30, 2001), 13.

[8] Center for Counterproliferation Research, *CBRN Terrorism: An Annotated Bibliography* (Washington, DC: National Defense University, May 2002), 3.

[9] W. Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, working paper (Washington, DC: Center for Counterproliferation Research, National Defense University, February 2001). See also Jonathan B. Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge, MA: MIT Press, 2000); Joshua Lederberg, ed., *Biological Weapons: Limiting the Threat* (Cambridge, MA: MIT Press, 1999).

[10] Milton Leitenberg, "An Assessment of the Biological Weapons Threat to the United States," *The Journal of Homeland Security*, January 2001.

[11] George J. Tenet, testimony to the Senate Select Committee on Intelligence on "The Worldwide Threat in 2000: Global Realities of Our National Security," February 2, 2000.

[12] U.S. Congress, Senate Committee on Appropriations, hearing on *Fiscal Year '03 Defense Department Appropriations*, 110th Congress, 2nd Session, May 21, 2002.

[13] Office of the Secretary of Defense, *Proliferation: Threat and Response* (Washington, DC: Government Printing Office, January 2001); U.S. Government, *The Worldwide Biological Warfare Weapons Threat* (Washington, DC: Government Printing Office, 2001), 1.

[14] Tenet, testimony to the Senate Foreign Relations Committee, March 21, 2000.

[15] Center for Counterproliferation Research, *The Counterproliferation Imperative: Meeting Tomorrow's Challenges* (Washington, DC: National Defense University, November 2001), 27.

[16] Ibid., 5–11. See also John F. Reichart, "Adversary Use of NBC Weapons: A Neglected Challenge," *Strategic Forum* 187 (Washington, DC: National Defense University, December 2001); and Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, eds., *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons* (Ithaca, NY: Cornell University Press, 2000).

[17] Department of Defense, *Quadrennial Defense Review Report*, 13–14. Capabilities-based planning focuses more on *how* an adversary could fight than on *whom* particular adversaries are or *where* conflict might occur.

[18] Donald A. Henderson before the Senate Foreign Relations Committee, September 5, 2002.

[19] White House, *The National Security Strategy of the United States of America* (Washington, DC: September 2002); White House, *National Strategy to Combat Weapons of Mass Destruction* (Washington, DC: December 2002). See also White House, *National Strategy for Homeland Security* (Washington, DC: July 2002).

[20] Center for Counterproliferation Research, *The Counterproliferation Imperative*, 49–51; Robert Kadlec, "Biological Deterrence in the 21st Century," unpublished manuscript, ANSER Institute for Homeland Security, 2002, 12–15. Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction* (Lexington: The University Press of Kentucky, 2001).

[21] George Bush and Brent Scowcroft, *A World Transformed* (New York: Knopf, 1998), 463; Colin L. Powell with Joseph E. Perisco, *My American Journey* (New York: Random House, 1995), 472, 485–486; James A. Baker III with Thomas M. Defrank, *The Politics of Diplomacy* (New York: G.P. Putnam's Sons, 1995), 359; H. Norman Schwarzkopf with Peter Petre, *General H. Norman Schwarzkopf: The Autobiography—It Doesn't Take A Hero* (New York: Bantam Books, 1992), 313.

[22] Center for Counterproliferation Research, *The Counterproliferation Imperative*, 50.

[23] General Accounting Office, *Biological Weapons: Efforts to Reduce Former Soviet Threat Offer Benefits, Poses New Risks*, GAO/NSIAD-00-138 (Washington, DC: General Accounting Office, April 2000), 27.

[24] John R. Bolton, remarks to the 5th Biological Weapons Convention RevCon Meeting, Geneva, Switzerland, November 19, 2001.

[25] General Accounting Office, *Biological Weapons,* 5.

[26] Ibid., 5, 14.

[27] For fiscal years 2000 through 2004, the executive branch plans to spend about $220 million to further engage former Soviet biological weapons institutes. See General Accounting Office, *Biological Weapons*, 27.

[28] White House, *National Strategy for Homeland Security*, 18.

[29] Bill Frist, "The Threat of Bioterrorism In America," committee statement, Senate Subcommittee on Public Health, Hearing on Bioterrorism, October 9, 2001.

[30] National Institute of Allergy and Infectious Disease (NIAID), National Institutes of Health, U.S. Department of Health and Human Services, NIAID Category A, B and C Priority Pathogens available in full at http://www.niaid.nih.gov/biodefense/bandc_priority.htm and Centers for Disease Control and Prevention, U.S. Department of Health and Human Services, Biological Diseases/Agents List, available in full at http://www.bt.cdc.gov/Agent/agentlist.asp.

[31] Thomas V. Inglesby, Rita Grossman, and Tara O'Toole, "A Plague on Your City: Observations from Topoff," *Clinical Infectious Disease* 32 (February 1, 2001), 436–445.

[32] Most vaccines are indicated for pre-exposure prophylactic use, but some can be successfully administered as a post-exposure prophylactic. Even fewer can be used for post-exposure treatment. Vaccinia virus, for example, can be used both as a pre-exposure and post-exposure prophylactic (to prevent the transmission of smallpox). It can also be used for post-exposure if it is administered within a few days of exposure to variola virus (the causative agent of smallpox).

[33] See Ken W. Alibek and Stephen Handelman, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World* (New York: Random House 1999).

[34] William Broad and Judith Miller, "Health Data Monitored for Bioterror Warning," *The New York Times*, January 27, 2003, A1.

[35] Donald H. Rumsfeld, prepared testimony, Senate Armed Services Committee, June 21, 2001.

[36] These include the Small Business Innovation Research, Small Business Technology Transfer, and Fast Track programs.

[37] White House, Statement by George W. Bush, "U.S. Will Meet WMD Threat with Confidence, Determination," Office of the Press Secretary, December 11, 2002.

John F. Reichart
Director

STAFF

W. Seth Carus
Senior Research Professor

Jason D. Ellis
Senior Research Professor

Rebecca K.C. Hersman
Senior Research Professor

Richard A. Love
Research Professor

Geoffrey D. Kiefer
Research Specialist

Todd M. Koca
Research Specialist

RECENT PUBLICATIONS

Anthrax in America: A Chronology and Analysis of the Fall 2001 Anthrax Attacks,
November 2002

CBRN Terrorism: An Annotated Bibliography,
May 2002

Possible Terrorist Use of Modern Biotechnology Techniques (FOUO),
April 2002

Defense by Other Means: The Politics of US-NIS Threat Reduction and Nuclear Security Cooperation
(Westport, CT: Praeger, 2001)

The Counterproliferation Imperative: Meeting Tomorrow's Challenges,
November 2001

Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century,
April 2001

For additional information, including publications information, please contact the center directly at CCRWebmaster@ndu.edu or (202) 685–4234 or visit the center Web site at: http://www.ndu.edu/centercounter/index.htm

Center for Counterproliferation Research
National Defense University
Fort Lesley J. McNair
Washington, DC